Raritan.

Dominion KSX II

ユーザ ガイド
リリース **2.3.0**

Copyright © 2010 Raritan, Inc.
DKSXII-v2.3.0-0E-J
2010 年 12 月
255-62-4030-00

本書には、著作権によって保護されている専有情報が含まれています。無断で転載することは禁じられており、本書のいかなる部分も、Raritan, Inc. より事前に書面による承諾を得ることなく複写、複製、他の言語へ翻訳することはできません。

© Copyright 2010 Raritan, Inc. 本書に記載されているサードパーティ製のすべてのソフトウェアおよびハードウェアは、それぞれの所有者の登録商標または商標であり、それぞれの所有者に帰属します。

FCC 情報

この装置は、FCC 規則のパート 15 に定められたクラス A デジタル装置に関する規制要件に基づき試験が実施され、その適合が認証されています。これらの規制要件は、商業環境において機器を使用する際、有害な干渉に対する妥当な保護を提供するために設けられています。この機器は、無線周波数エネルギーを生成かつ利用すると共に、放射することもあります。取扱説明書に従って設置および使用が行われない場合は、無線通信に有害な干渉を引き起こす恐れがあります。この機器を住宅地で利用すると有害な干渉を引き起こす場合もあります。

VCCI 情報 (日本)

この装置は，クラスA情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。 VCCI－A

Raritan は、事故、災害、誤用、乱用、本製品の Raritan 製品以外への改良が起因する、または Raritan が適切にコントロールできないような状況下、もしくは通常の操作以外で発生した本製品への損傷に対して一切責任を負いません。

本製品に付属されている電源ケーブルは、本製品でのみ使用してください。

1F61
I.T.E.

目次

はじめに 1

KSX II の概要 2
ヘルプでの最新情報....... 4
KSX II ヘルプ 5
関連文書 5
KSX II のクライアント アプリケーション 6
仮想メディア 6
製品の写真 7
製品の特長 8
ハードウェア 8
ソフトウェア 9
外部製品の概要....... 9
用語 12
パッケージの内容 14

インストールと設定 16

概要....... 16
デフォルトのログイン情報....... 16
入門....... 17
手順 1: KVM ターゲット サーバの設定 17
ステップ 2: ネットワーク ファイアウォールの設定 28
ステップ 3: 装置の接続....... 29
手順 4: KSX II の設定....... 34
手順 6: キーボード言語の設定（オプション）....... 42

ターゲット サーバの使用 44

インタフェース....... 44
KSX II ローカル コンソール: KSX II デバイス....... 45
KSX II リモート コンソール インタフェース 46
MPC、VKC、および AKC と組み合わせて使用する場合のプロキシ サーバ設定 59
Virtual KVM Client (VKC)....... 61
Raritan Virtual KVM Client について....... 61
KVM ターゲット サーバへの接続....... 61
ツール バーのボタンおよびステータス バーのアイコン 62
KVM ターゲット サーバの切り替え 64
ターゲット サーバの電源管理....... 65
KVM ターゲット サーバの切断....... 66

Raritan.

USB プロファイルの選択 66
[Connection Properties] (接続プロパティ) 67
接続情報 69
キーボードのオプション 70
ビデオのプロパティ 74
マウス オプション 78
VKC 仮想メディア 83
スマート カード 84
ツール オプション 87
表示オプション 90
バージョン情報 - Virtual KVM Client 91
Active KVM Client (AKC) 91
概要 92
AKC でサポートされている .NET Framework、オペレーティング システムとブラウザ 92
AKC を使用するための必要条件 93
Multi-Platform Client (MPC) 94
Web ブラウザからの MPC の起動 94
Raritan Serial Console (RSC) 95
リモート コンソールから RSC を開く 95

ラック PDU (電源タップ) のコンセントの制御 97

概要 97
コンセントの電源オン/オフの切り替えまたは電源再投入を行う 98

仮想メディア 100

概要 101
仮想メディアを使用するための条件 104
Windows 環境での VKC および AKC を介した仮想メディア 106
仮想メディアの使用 107
仮想メディア ファイル サーバのセットアップ (ファイル サーバ ISO イメージの場合のみ) 109
仮想メディアへの接続 111
[Local Drives] (ローカル ドライブ) 111
読み取り/書き込み可能に設定できない状況 112
CD-ROM/DVD-ROM/ISO イメージ 113
仮想メディアの切断 114

USB プロファイル 115

概要 115
CIM の互換性 116
使用できる USB プロファイル 116
KVM ポート用のプロファイルの選択 123
Mac のブート メニュー使用時のマウス モード 123

User Management 124

ユーザ グループ ... 124
ユーザ グループ リスト ... 125
ユーザとグループの関係 ... 125
新規ユーザ グループの追加 ... 126
既存のユーザ グループの変更 ... 131
ユーザ ... 132
KSX II ユーザ リストの表示 ... 132
新規ユーザの追加 ... 132
既存のユーザ グループの変更 ... 133
KSX II からのユーザのログオフ (強制ログオフ) ... 134
[Authentication Settings] (認証設定) ... 134
LDAP/LDAPS リモート認証の実装 ... 135
ユーザ グループ情報を Active Directory サーバから返す ... 139
RADIUS リモート認証の実装 ... 140
ユーザ グループ情報を RADIUS 経由で返す ... 143
RADIUS 通信交換仕様 ... 143
ユーザ認証プロセス ... 145
パスワードの変更 ... 146

デバイス管理 147

ネットワーク設定 ... 147
ネットワーク基本設定 ... 148
LAN インタフェース設定 ... 152
[Device Services] (デバイス サービス) ... 153
Telnet 接続を有効にする ... 153
SSH を有効にする ... 154
HTTP ポートおよび HTTPS ポートの設定 ... 154
検出ポートを入力する ... 155
シリアル コンソール アクセスを有効にする ... 155
URL を経由したダイレクト ポート アクセスの有効化 ... 156
Telnet、IP アドレス、または SSH 経由のダイレクト ポート アクセスの構成 ... 157
AKC ダウンロード サーバ証明書の検証の有効化 ... 159
モデムを設定する ... 160
日付/時刻の設定 ... 162
イベント管理 ... 162
[Event Management Settings] (イベント管理設定) の設定 ... 163
[Event Management - Destinations] (イベント管理 - 送信先) の設定 ... 165
ポートの設定 ... 169
電源制御 ... 171
ターゲットの設定 ... 173
ブレード シャーシの設定 ... 174

USB プロファイルの設定 ([Port] (ポート) ページ) 199
KSX II のローカル ポートの設定 201
ポート キーワード 204
ポート グループ管理 206

セキュリティの管理 207

セキュリティの設定 207
[Login Limitations] (ログイン制限) 208
[Strong Passwords] (強力なパスワード) 210
[ユーザ ブロック] 211
[Encryption & Share] (暗号化および共有) 213
FIPS 140-2 の有効化 217
IP アクセス制御を設定する 219
SSL 証明書 221
セキュリティ バナー 224

保守 227

メンテナンス機能 (ローカル/リモート コンソール) 227
[Audit Log] (監査ログ) 228
[Device Information] (デバイス情報) 229
バックアップと復元 230
[USB Profile Management] (USB プロファイルの管理) 233
プロファイル名の競合を処理する 234
CIM アップグレード 234
[Upgrading Firmware] (ファームウェアのアップグレード) 235
[Upgrade History] (アップグレード履歴) 238
KSX II の再起動 238
CC Unmanage 239
CC-SG 管理の終了 240

診断 242

[Network Interface] (ネットワーク インタフェース) ページ....242
[Network Statistics] (ネットワーク統計) ページ....243
[Ping Host] (ホストに ping する) ページ....245
[Trace Route to Host (ホストへのルートの追跡)] ページ....245
[KSX II Diagnostics] (KSX II 診断) ページ....246

コマンド ライン インタフェース (CLI) 249

概要....250
CLI を使用しての KSX II へのアクセス....251
KSX II への SSH 接続....251
Windows PC からの SSH アクセス....251
UNIX/Linux ワークステーションからの SSH アクセス....252
KSX II への Telnet 接続....252
Telnet 接続を有効にする....252
Windows PC から Telnet で接続する....252
KSX II へのローカル シリアル ポート接続....253
ポート設定....253
ログオン....253
CLI の画面操作....255
コマンドのオート コンプリート....255
CLI 構文: ヒントとショートカット キー....256
すべての CLI レベルで使用できるコマンド....256
CLI を使用した初期設定....257
パラメータ値を設定する....257
ネットワーク パラメータの設定....257
CLI プロンプト....258
CLI コマンド....258
セキュリティ上の問題....259
ターゲット接続と CLI....259
ターゲットでのエミュレーションの設定....259
CLI を使用したポート共有....260
KSX II コンソール サーバ設定用コマンドを使用する....260
ネットワークを設定する....260
interface コマンド....261
name コマンド....262
connect コマンド....262
ipv6 コマンド....263

KSX II ローカル コンソール 264

概要....264
KSX II ローカル コンソールを使用する....265
ユーザが同時接続可能....265
KSX II ローカル コンソール インタフェース....265
セキュリティと認証....266
ローカル コンソールのスマート カード アクセス....267
ローカル コンソールの USB プロファイル オプション....268
有効な解像度....269
[Port Access] (ポート アクセス) ページ (ローカル コンソール サーバ ディスプレイ)....270
サーバ表示....272
ホット キーと接続キー....273
接続キーの例....273
各言語に対して KSX II でサポートされているキーボード....274
Sun サーバへのアクセス時に使用できる特別なキー組み合わせ....276
ターゲット サーバにアクセスする....276
KSX II ローカル コンソールの画面に切り替える....277
ローカル ポートの管理....277
KSX II ローカル コンソールの [Local Port Settings] (ローカル ポート設定) ページ....277
KSX II ローカル コンソールの [Factory Reset] (出荷時設定にリセット) ページ....280
リセット ボタンを使用して KSX II をリセットする....282

モデム設定 283

UNIX、Linux、および MPC 向け認定モデム....283
低帯域幅の KVM 設定....284
クライアント ダイヤルアップ ネットワーク設定....285
Windows 2000 のダイヤルアップ ネットワーク設定....285
Windows Vista のダイヤルアップ ネットワーク設定....289
Windows XP のダイヤルアップ ネットワーク設定....290

仕様 297

物理的仕様....297
サポートされているオペレーティング システム (クライアント)....298
サポートされているオペレーティング システムおよび CIM (KVM ターゲット サーバ)....299
サポートされているブラウザ....302
コンピュータ インタフェース モジュール (CIM)....302
サポートされている Paragon II CIMS および設定....303
KSX II - KSX II 構成の Paragon CIM に関するガイドライン....304
KSX II - Paragon II 構成に関するガイドライン....305

サポートされている画面解像度 307
KSX II ローカル コンソールでサポートされる言語 308
使用される TCP ポートおよび UDP ポート 308
スマート カード リーダー 310
サポートされているスマート カード リーダーとサポートされていないスマート カード リーダー 310
スマート カードの最小システム要件 311
環境要件 313
緊急時の接続 314
電気的仕様 314
サポートされているリモート接続 315
KVM プロパティ 315
使用されるポート 315
サポートされているターゲット サーバとビデオ 317
シリアル デバイスの距離 317
ネットワーク速度の設定 318
接続 319
KSX II のシリアル RJ-45 ピン配列 320
DB9F Null 化シリアルアダプタのピン配列 321
DB9M Null 化シリアルアダプタのピン配列 321
DB25F Null 化シリアルアダプタのピン配列 322
DB25M Null 化シリアルアダプタのピン配列 322

LDAP/LDAPS スキーマの更新 324

ユーザ グループ情報を返す 324
LDAP/LDAPS から返す場合 324
Microsoft Active Directory から返す場合 325
スキーマへの書き込み操作を許可するようにレジストリを設定する 325
新しい属性を作成する 326
属性をクラスに追加する 327
スキーマ キャッシュを更新する 328
ユーザ メンバの rciusergroup 属性を編集する 329

留意事項 332

概要 332
Java 332
AES (256 ビット) を使用する際の前提条件と Java のサポート対象構成 332
Java Runtime Environment (JRE) 333
オペレーティング システムの IPv6 のサポートに関する留意事項 335
キーボード 336
アメリカ英語以外のキーボード 336
Macintosh キーボード 339

Dell 筐体を接続する場合のケーブル長と画面解像度 339
ブラウザに関する留意事項..... 340
Fedora Core のフォーカスに関する問題を解決する 340
マウス ポインタの同期 (Fedora) 340
Fedora サーバへの VKC および MPC のスマート カード接続..... 340
Fedora 使用時の Firefox のフリーズに関する問題の解決..... 341
USB ポートおよびプロファイルに関する留意事項 341
VM-CIM および DL360 の USB ポート 341
USB プロファイルの選択に関するヘルプ..... 341
スマート カード リーダー使用時の USB プロファイルの変更 343
SUSE と VESA のビデオ モード 343
CIM に関する留意事項..... 344
Linux ターゲット サーバに対して Windows の 3 ボタン マウスを使用する場合..... 344
仮想メディアに関する留意事項 344
Dell OptiPlex および Dimension コンピュータ 344
Windows 2000 の仮想メディアへのアクセス 344
ファイル追加後に仮想メディアが最新の情報に更新されない 344
仮想メディア機能利用時におけるターゲット サーバの BIOS の起動時間..... 344
高速の仮想メディア接続を使用した場合の仮想メディアの接続エラー..... 345
CC-SG に関する留意事項..... 345
VKC のバージョンが CC-SG プロキシ モードで認識されない 345
シングル マウス モード: CC-SG の管理下にあるターゲットに接続する場合..... 345
デバイスのポート間の移動 345

FAQ 346

全般的な質問 347
シリアル アクセス 349
ユニバーサル仮想メディア 355
USB プロファイル 356
IPv6 ネットワーキング 358
リモート アクセス 360
Ethernet と IP ネットワーキング 362
サーバ 366
ブレード サーバ 366
インストール 369
ローカル ポート 371
電源制御 373
拡張性 374
セキュリティ 375
スマート カード認証と CAC 認証 377
管理機能 378
その他 379

索引 381

Ch 1　はじめに

この章の内容

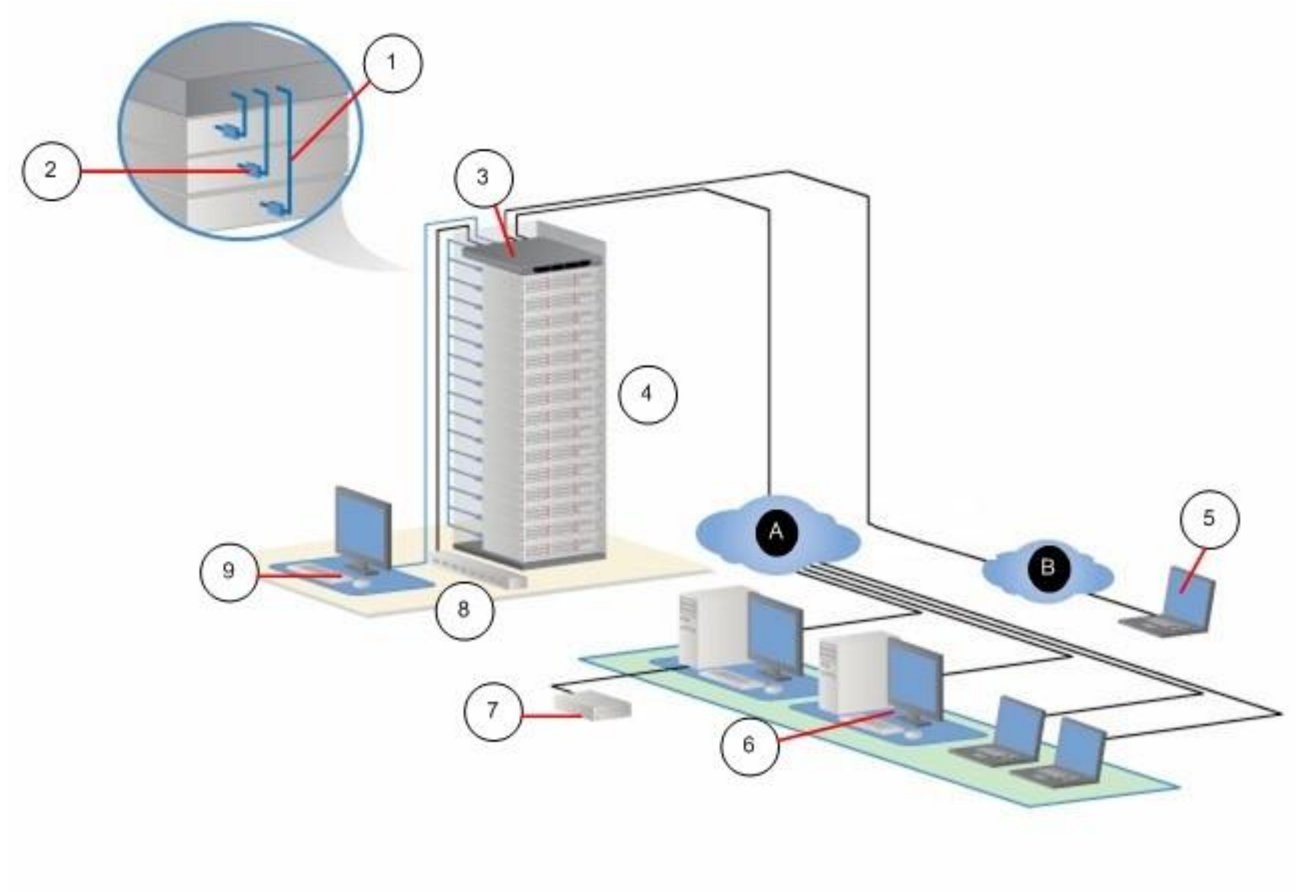
KSX II の概要......2
ヘルプでの最新情報......4
KSX II ヘルプ......5
KSX II のクライアント アプリケーション......6
仮想メディア......6
製品の写真......7
製品の特長......8
外部製品の概要......9
用語......12
パッケージの内容......14

KSX II の概要

Raritan の Dominion KSX II は、企業規模のセキュアなデジタル デバイスで、世界中どこからでも Web ブラウザを介してリモート KVM (キーボード、ビデオ、マウス) サーバ アクセスやシリアル デバイス管理、および電源管理を行うことができる統合的なソリューションを提供します。ラック内の KSX II で、1 組のキーボード、モニタ、およびマウスからすべての KVM サーバおよびシリアル ターゲットを制御できます。また、1 つのローカル シリアル ポートからすべてのシリアル ターゲットへのアクセスと制御を行うこともできます。KSX II のリモート アクセス機能の統合によって、Web ブラウザを使用したサーバのフル アクセスおよび制御が可能になっています。

KSX II は、標準 UTP (Cat 5/5e/6) ケーブルを使用した配線で簡単に取り付けることができます。その高度な機能には、仮想メディア、最大で 256 ビットの暗号化、リモート電源管理、二重化 Ethernet、LDAP、RADIUS、Active Directory®、Syslog との統合、および Web 管理などが含まれています。これらの機能により、より高いアップタイム、より優れた生産性、強固なセキュリティを、いつどこからでも提供できます。

KSX II 製品は、スタンドアロン装置として動作し、中央管理デバイスには依存しません。大規模なデータ センターや企業では、複数の KSX II デバイスを、Raritan の CommandCenter Secure Gateway (CC-SG) 管理ユニットを使用することで、他の Raritan デバイスとともに 1 つの論理ソリューションとして統合できます。



図の説明			
1	Cat5 ケーブル	7	リモート仮想メディア USB ドライブ
2	コンピュータ インタフェース モジュール (CIM)	8	ラック PDU (電源タップ)
3	KSX II	9	ローカル アクセス
4	リモート KVM および シリアル デバイス	A	IP LAN/WAN
5	モデム アクセス	B	PSTN
6	リモート（ネットワーク）アクセス		

ヘルプでの最新情報

製品やユーザ マニュアルに対する強化や変更に基づいて、以下の情報が追加されています。

- KSX II によって使用される HTTP ポートまたは HTTPS ポートを設定できるようになりました。 詳細については、「*HTTP ポートおよび HTTPS ポートの設定* 『*154*p. 』」を参照してください。
- KSX II の、スマート カード リーダーの新たなサポートに関する情報がヘルプに追加されました。「*スマート カード* 『*84*p. 』」および「*スマート カード リーダー* 『*310*p. 』」を参照してください。
- セキュリティ バナー機能が追加されました。これにより、セキュリティ バナーを作成および表示できます。また、KSX II ログイン プロセスで、セキュリティ同意書に同意するかどうかの選択をユーザに求めることもできます。詳細については、「*セキュリティ バナー* 『*224*p. 』」を参照してください。
- KSX II には、FIPS 140-2 で検証された暗号化モジュールが埋め込まれるようになりました。「*暗号化および共有* 『*213*p. の"*[Encryption & Share] (暗号化および共有)*"参照 』」を参照してください。
- KSX II では P2CIM-APS2DUAL CIM および P2CIM-AUSBDUAL CIM がサポートされています。これらの CIM を使用した場合、RJ45 で 2 台の異なる KVM スイッチに接続できます。 詳細については、「*サポートされている Paragon CIMS および設定* 『*303*p. の"*サポートされている Paragon II CIMS および設定*"参照 』」を参照してください。
- ブラウザからターゲットに直接接続できるダイレクト ポート アクセス機能が KSX II に追加されました。「*デバイス サービス* 『*153*p. の"*[Device Services] (デバイス サービス)*"参照 』」を参照してください。
- Active KVM Client が KSX II でサポートされるようになりました。「*Active KVM Client (AKC)* 『*91*p. 』」を参照してください。
- USB プロファイルが KSX II でサポートされるようになりました。「*USB プロファイル* 『*115*p. 』」を参照してください。
- KSX II に追加のワイド画面解像度のサポートが追加されました。「*サポートされている画面解像度* 『*307*p. 』」を参照してください。
- [Port Access] (ポート アクセス) ページに新しいタブが追加されました。このタブではサーバを名前で検索できます。詳細については、「*[Port Access] (ポート アクセス) ページ* 『*51*p. 』」を参照してください。
- KSX II で Microsoft の Windows 7® オペレーティング システムがサポートされるようになりました。「*サポートされているオペレーティング システム (クライアント)* 『*298*p. 』」および「*サポートされているオペレーティング システムおよび CIM (KVM ターゲット サーバ)* 『*299*p. 』」を参照してください。

- ユーザをログオフできるようになりました (強制ログオフ)。「*ユーザのログオフ (強制ログオフ)*『*134*p. の"*KSX II からのユーザのログオフ (強制ログオフ)*"参照 』」を参照してください。

このデバイスおよびこのバージョンのヘルプに対して適用される変更の詳細は、リリース ノートを参照してください。

KSX II ヘルプ

KSX II ヘルプでは、KSX II のインストール、セットアップ、および設定の方法に関する情報を確認できます。また、ターゲット サーバに対するアクセス、仮想メディアの使用、ユーザおよびセキュリティの管理、KSX II の保守と診断に関する情報も提供します。

現在のリリースに関する重要な情報について KSX II リリースノートを参照してから、KSX II を使用してください。

PDF バージョンのヘルプは、Raritan の Web サイトの [Firmware and Documentation] ページからダウンロードできます。最新のユーザ ガイドが利用できるかどうかを Raritan の Web サイトで確認することをお勧めします。

オンライン ヘルプを使用するには、ブラウザでアクティブ コンテンツを有効にする必要があります。Internet Explorer 7 を使用している場合、スクリプトレットを有効にする必要があります。これらの機能を有効にする方法については、ブラウザのヘルプを参照してください。

関連文書

KSX II ヘルプには、KSX II クイック セットアップ ガイドが付属しています。これは、*Raritan の Web サイト*『*http://www.raritan.com/support/firmware-and-documentation* 参照 』の [Firmware and Documentation] ページにあります。

KSX II で使用するクライアント アプリケーションのインストールの要件および手順についても、Raritan の Web サイトにある『KVM and Serial Access Clients Guide』を参照してください。該当する場合は、KSX II で使用される特定のクライアント機能がこのヘルプに掲載されます。

KSX II のクライアント アプリケーション

KSX II で使用できるクライアント アプリケーションは以下のとおりです。

- Virtual KVM Client (VKC)
- Active KVM Client (AKC)
- Multiplatform Client (MPC)
- Raritan Serial Console (RSC)

クライアント アプリケーションの詳細については、『KVM and Serial Access Clients User Guide』を参照してください。このガイドの「***ターゲット サーバの使用***『*44*p. 』」セクションも参照してください。KSX II でのクライアントの使用に関する情報が記載されています。

注: MPC および VKC を使用するには、Java™ Runtime Environment (JRE™) が必要です。AKC は .NET ベースです。

仮想メディア

すべての KSX II モデルにおいて仮想メディアがサポートされています。これにより、仮想メディアのメリット（ソフトウェアのインストールおよび診断をサポートするためにターゲット サーバにリモート ドライブ/メディアをマウントすること）がすべての KSX II モデルにもたらされます。仮想メディア セッションは、128 ビットおよび 256 ビット AES または RC4 暗号化によって保護できます。

それぞれの KSX II は仮想メディアを装備しているので、CD、DVD、USB、内蔵およびリモート ドライブ、イメージなどのいろいろなデバイスを使用したリモート管理タスクが可能です。他のソリューションとは異なり、KSX II は、ハード ディスク ドライブおよびリモートにマウントされたイメージの仮想メディア アクセスをサポートして、高い柔軟性と生産性を提供します。

新しい D2CIM-VUSB および D2CIM-DVUSB CIM (コンピュータ インタフェース モジュール) では、USB 2.0 インタフェースをサポートする KVM ターゲット サーバへの仮想メディア セッションがサポートされます。また、この新しい CIM では、Absolute Mouse Synchronization やリモート ファームウェア更新もサポートされます。

注: DVUSB CIM の黒のコネクタは、キーボードとマウスに使用します。グレーのコネクタは、仮想メディアに使用します。CIM の両方のプラグをデバイスに接続したままにします。両方のプラグがターゲット サーバに接続されていない場合は、デバイスが正しく動作しないことがあります。

製品の写真

KSX II 144 および 188

CIM

シリアル アダプタ

製品の特長

ハードウェア

- KVM および IP 上のシリアル リモート アクセス
- 1U サイズ、ラックマウント対応 (ブラケット付属)
- DKSX2-144 – 4 シリアル/4 KVM サーバ ポート
- DKSX2-188 – 8 シリアル/8 KVM サーバ ポート
- 8 ユーザ (複数シリアル ユーザ) により共有可能な 1 KVM チャネル
- UTP (Cat5/5e/6) ケーブルを使用したサーバへの配線
- フェイルオーバ対応の二重化 Ethernet ポート (10/100/1000 LAN)
- フィールド アップグレード可能
- ラック内アクセス用ローカル KVM ポート
  - サポートされる USB デバイス用の、USB 2.0 ポート (前面に 1 基、背面に 3 基)
  - リモート ユーザ アクセスと同時に操作可能
  - 管理用のローカル グラフィカル ユーザー インターフェース (GUI)
  - KVM とシリアル ターゲットはどちらも KVM ローカル ポートで接続可能
- CLI ベースの管理およびシリアル ターゲット アクセス用の、ローカル シリアル ポート (RS232)
- 電源管理の統合
- 二重化専用電源制御ポート
- ネットワーク アクティビティやリモート KVM ユーザの状況を示す LED インジケータ
- ハードウェア リセット ボタン
- 内蔵モデム
- 中央管理されるアクセス セキュリティ

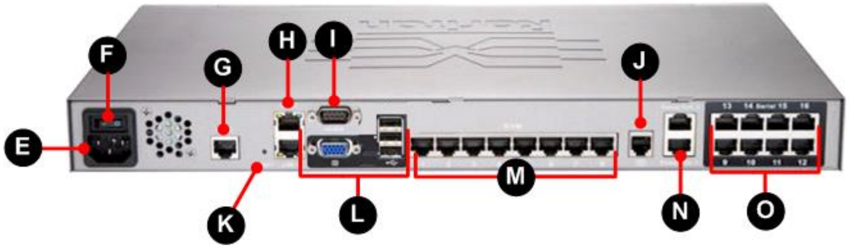
ソフトウェア

- 仮想メディア（D2CIM-VUSB CIM および D2CIM-DVUSB CIM により提供）
- ずれないマウス（Absolute Mouse Synchronization）(D2CIM-VUSB CIM および D2CIM-DVUSB CIM により提供)
- プラグ & プレイ
- Web ベースのアクセスと管理
- わかりやすいグラフィカル ユーザ インタフェース（GUI）
- すべての KVM 信号を 256 ビット暗号化（ビデオや仮想メディアを含む）
- LDAP/LDAPS、Active Directory®、RADIUS、または内部機能によるローカル認証および認可
- DHCP または静的な IP アドレスの指定
- スマート カード/CAC 認証
- SNMP および Syslog 管理
- IPv4 および IPv6 のサポート
- 誤操作を防ぐためにサーバと直接関連付けられる電源管理
- Raritan の CommandCenter Secure Gateway (CC-SG) 管理本体との統合
- CC-SG の制御からデバイスを解除するための CC Unmanage 機能

外部製品の概要

以下の図は、KSX II の外部コンポーネントを示しています。KSX II 144 には、KVM ポートとシリアル ポートがそれぞれ 4 つあり、図で使用されている KSX II 188 には、KVM ポートとシリアル ポートがそれぞれ 8 つあることに注意してください。

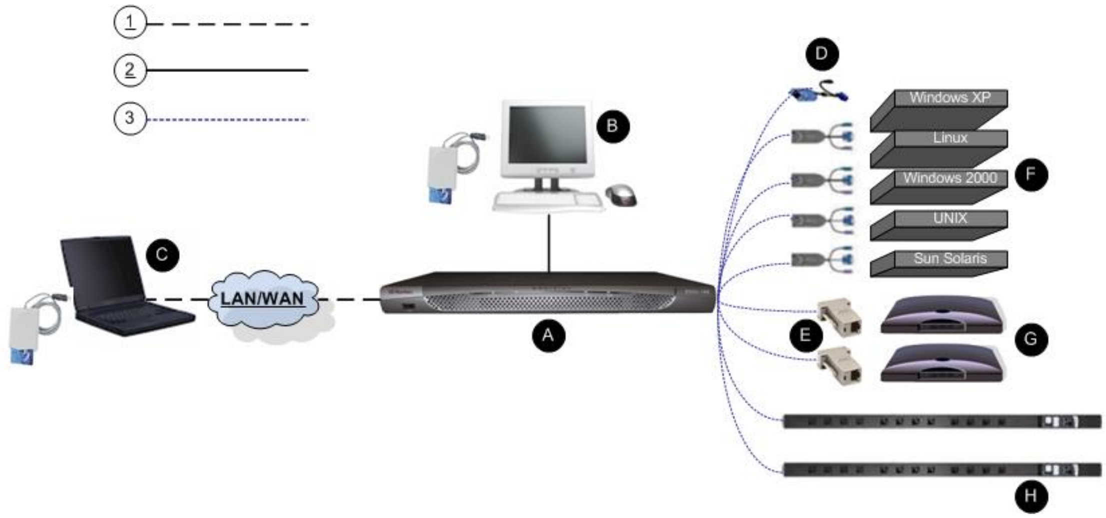
品目	説明
A	USB ポート
B	リモート インジケータ ランプ
C	LAN1 および LAN2 インジケータ ランプ
D	電源インジケータ ランプ



品目	説明
E	AC 電源コード プラグ 詳細は、「***電源管理*** 『*171*p. の"***電源制御***"参照先 』」を参照してください。
F	電源オン/オフ スイッチ
G	LAN 3 ポート *注: LAN 3 ポートは、将来用に予約されています。*
H	LAN1 および LAN2 ポート 装置の接続方法の詳細は、「***手順 3: 装置の接続*** 『*29*p. の"***ステップ 3: 装置の接続***"参照 』」を参照してください。
I	管理ポート 装置の接続方法の詳細は、「***手順 3: 装置の接続*** 『*29*p. の"***ステップ 3: 装置の接続***"参照 』」を参照してください。
J	外部モデム ポート 詳細は、「***モデムの設定*** 『*283*p. の"***モデム設定***"参照先 』」を参照してください。
K	リセット ボタン 詳細については、「***リセット ボタンを使用して KSX II をリセットする*** 『*282*p. 』」を参照してください。
L	ローカル ポート 装置の接続方法の詳細は、「***手順 3: 装置の接続*** 『*29*p. の"***ステップ 3: 装置の接続***"参照 』」を参照してください。
M	KVM ポート 装置の接続方法の詳細は、「***手順 3: 装置の接続*** 『*29*p. の"***ステップ 3: 装置の接続***"参照 』」を参照してください。
N	電源制御 1 および電源制御 2 詳細は、「***電源管理*** 『*171*p. の"***電源制御***"参照先 』」を参照してください。
O	シリアル ポート 装置の接続方法の詳細は、「***手順 3: 装置の接続*** 『*29*p. の"***ステップ 3: 装置の接続***"参照 』」を参照してください。

用語

このマニュアルでは、KSX II の典型的な構成コンポーネントを示すにあたり、以下の用語を使用します。



図の説明	
1	TCP/IP IPv4 または IPv6
2	KVM (キーボード、ビデオ、マウス)
3	UTP ケーブル (Cat5/5e/6)
A	KSX II
B	**ローカル アクセス コンソール** ローカル ユーザ － KVM ターゲット サーバおよびシリアル ターゲットをローカルに (ネットワーク経由ではなく直接ラック内で) 制御するために KSX II に直接接続された、(キーボード、マウス、マルチシンク VGA モニタで構成される) オプションのユーザ コンソール。USB スマート カード リーダーをローカル ポートに接続してターゲット サーバにマウントすることもできます。 ローカル管理者 － ローカル管理ポートを使用して KSX II をワークステーションに直接接続し、シリアル ターゲットを管理したり、HyperTerminal などのターミナル エミュレーション プログラムを使用してシステムを設定したりできます。ローカル管理ポートでは、標準のヌル モデム ケーブルを使用する必要があります。
C	**リモート PC** KSX II に接続している KVM ターゲット サーバおよびシリアル ターゲットへのアクセスとその制御に使用する、ネットワークに接続したコンピュータ。KSX II によってリモートでサポートされるオペレーティング システムの一覧については、「サポートされているオペレーティング システム (クライアント)」を参照してください。
D	CIM 各ターゲット サーバに接続するドングル。サポートされているすべてのオペレーティング システムに対して使用できます。KSX II でサポートされている CIM については、「サポートされている CIM」を参照してください。
E	**シリアル アダプタ** シリアル ケーブルを接続するアダプタ。
F	**ターゲット サーバ** KVM ターゲット サーバ － KSX II を介してリモート接続され

図の説明	
	る、ビデオ カードとユーザ インタフェースを備えたサーバ (Windows®、Linux®、Solaris™ など)。サポートされているオペレーティング システムおよび CIM については、「サポートされているオペレーティング システムおよび CIM (ターゲット サーバ)」を参照してください。 シリアル ターゲット – KSX II を介してリモート接続されるシリアル ポートを持つサーバ、ルータ、およびスイッチ。
G	ルータ
H	Dominion PX ラック PDU (電源タップ) KSX II を介してリモート アクセスされる Raritan ラック PDU。

パッケージの内容

KSX II は、標準 1U 19 インチ ラックマウント シャーシに搭載される、完全に構成されたスタンドアロン製品として出荷されます。各 KSX II デバイスは、以下の内容で出荷されます。

数量	品目
1	Dominion KSX II デバイス
1	Dominion KSX II クイック セットアップ ガイド
1	ラックマウント キット
1	AC 電源コード。同梱された電源ケーブルは、本製品専用に使われるものです。
1	Cat5 ネットワーク ケーブル
1	Cat5 ネットワーク クロスケーブル
1	ゴム足一組（4 個、デスクトップ用）
1	アプリケーション ノート
1	保証書
1	電話線ケーブル
1	ループバック アダプタ

Ch 2　インストールと設定

この章の内容

概要..16
デフォルトのログイン情報...16
入門..17

概要

このセクションでは、インストール手順の概要を説明します。それぞれの手順については、この章の後のセクションで詳しく説明します。

KSX II をインストールおよび設定するには、以下の手順に従います。

- *手順 1: KVM ターゲット サーバの設定* 『17p. 』
- *手順 2: ネットワーク ファイアウォールの設定* 『28p. の"*ステップ 2: ネットワーク ファイアウォールの設定*"参照 』
- *手順 3: 装置の接続* 『29p. の"*ステップ 3: 装置の接続*"参照 』
- *手順 4: KSX II* 『34p. の"*手順 4: KSX II の設定*"参照 』 の設定
- *手順 5 (オプション): キーボード言語の設定* 『42p. の"*手順 6: キーボード言語の設定 (オプション)*"参照 』

初期構成には、デフォルトの IP アドレス、ユーザ名、およびパスワードが必要です。「*デフォルトのログイン情報* 『16p. 』」を参照してください。

デフォルトのログイン情報

デフォルト設定	値
ユーザ名	*admin* このユーザは、管理者特権を有します。
パスワード	*(「raritan」) を入力します。* KSX II を初めて起動したときは、デフォルトのパスワードを変更する必要があります。
IP アドレス	192.168.0.192.

重要: バックアップと事業の継続性のためには、バックアップ管理者用のユーザ名およびパスワードを作成し、その情報を安全な場所に保管しておくことを強くお勧めします。

入門

手順 1: KVM ターゲット サーバの設定

KVM ターゲット サーバとは、KSX II を介してアクセスおよび制御するコンピュータのことです。最適なパフォーマンスを確保するために、KSX II をインストールする前に、すべての KVM ターゲット サーバを設定します。この設定は、KVM ターゲット サーバのみに適用されます。KSX II のリモート アクセスに使用されるクライアント ワークステーション（リモート PC）には適用されません。詳細については、「**用語**」を参照してください。

デスクトップの背景

Windows®、Linux®、X-Windows、Solaris™、KDE などのグラフィカル ユーザ インタフェースを実行する KVM ターゲット サーバは、帯域幅効率とビデオ パフォーマンスを最適化するための設定が必要になる場合があります。デスクトップの背景は完全な無地にする必要はありませんが、写真や複雑な配色の背景を使用すると、パフォーマンスが低下する可能性があります。

マウスの設定

KSX II は、ずれないマウス モード™、インテリジェント マウス モード、および標準マウス モードで動作します。

ずれないマウス モードの場合は、マウス パラメータを変更する必要はありません。ただし、このモードを使用するには、D2CIM-VUSB、D2CIM-DVUSB、またはデジタル CIM が必要です。標準マウス モードとインテリジェント マウス モードの場合は、マウス パラメータを特定の値に設定する必要があります。マウス設定は、ターゲットのオペレーティング システムによって異なります。詳細については、使用するオペレーティング システムのマニュアルを参照してください。

インテリジェント マウス モードは、ほとんどの Windows プラットフォームで正常に機能しますが、ターゲット上でアクティブ デスクトップが設定されている場合は、予測できない結果を生じることがあります。インテリジェント マウス モードではアニメーション カーソルは使用しないでください。 インテリジェント マウス モード設定の詳細については、「*インテリジェント マウス モード*『*81*p. 』」を参照してください。

ブレード筐体内に KVM スイッチを備えているサーバの場合、通常、ずれないマウス機能はサポートされません。

オペレーティング システムのマウスとビデオの設定

このセクションでは、ターゲット サーバ上で使用されているオペレーティング システムに固有のビデオ モードとマウスについて説明します。

Windows XP、Windows 2003、および Windows 2008 の設定

▶ **Windows XP®、Windows 2003®、および Windows 2008® を実行している KVM ターゲット サーバを設定するには、以下の手順に従います。**

1. マウスの設定を行います。
   a. [スタート]、[コントロール パネル]、[マウス] の順に選択します。
   b. [ポインタ オプション] タブをクリックします。
   c. [速度] グループで、以下の操作を行います。
      - ポインタの速度設定をちょうど中間の速度に設定します。
      - [ポインタの精度を高める] チェック ボックスをオフにします。
      - [動作] のオプションを無効にします。
      - [OK] (OK) をクリックします。
2. アニメーション効果を無効にします。
   a. [コントロール パネル] の [画面] オプションを選択します。
   b. [デザイン] タブをクリックします。
      - [効果] ボタンをクリックしてます。
      - [次のアニメーション効果をメニューとヒントに使用する] オプションをオフにします。
3. [OK] をクリックして、[コントロール パネル] を閉じます。

注: Windows XP、Windows 2000、または Windows 2008 を実行している KVM ターゲット サーバの場合、KSX II を介したリモート接続用に、専用のユーザ名を作成することが可能です。これにより、ターゲット サーバのマウス ポインタの速度や加速を KSX II 接続用に遅く設定できます。

Windows XP、2000、および 2008 のログイン ページでは、マウスのパラメータが、最適な KSX II パフォーマンス用に提案されたパラメータとは異なる、プリセットされたパラメータに戻ります。この結果、これらの画面ではマウスの同期は最適ではありません。

注: Windows KVM ターゲット サーバのレジストリを調整してもかまわない場合のみ、次の操作を行ってください。Windows レジストリ エディタを使って次の設定を変更することにより、ログイン ページで KSX II のマウスの同期を改善することができます。
HKey_USERS¥.DEFAULT¥Control Panel¥Mouse:> MouseSpeed = 0、MouseThreshold 1=0、MouseThreshold 2=0。

Windows 7 および Windows Vista の設定

Windows Vista® を実行している KVM ターゲット サーバを設定するには、以下の手順に従います。

1. マウスの設定を行います。
   a. ［スタート］、［設定］、［コントロール パネル］、［マウス］の順に選択します。
   b. 左側のナビゲーション パネルから［システムの詳細設定］を選択します。［システムのプロパティ］ダイアログ ボックスが表示されます。
   c. ［ポインタ オプション］タブをクリックします。
   d. ［速度］グループで、以下の操作を行います。
      - ポインタの速度設定をちょうど中間の速度に設定します。
      - ［ポインタの精度を高める］チェック ボックスをオフにします。
      - ［OK］をクリックします。
2. アニメーション効果とフェード効果を無効にします。
   a. ［コントロール パネル］の［システム］オプションを選択します。
   b. ［パフォーマンス情報］を選択し、［ツール］、［詳細ツール］、［調整］の順に選択し、Windows の外観とパフォーマンスを調整します。
   c. ［詳細設定］タブをクリックします。
   d. ［パフォーマンス］グループの［設定］をクリックして、［パフォーマンス オプション］ダイアログ ボックスを開きます。
   e. ［カスタム］オプションで、以下のチェック ボックスをオフにします。
   - アニメーション関連のオプション:
      - ［Windows 内のアニメーション コントロールと要素］
      - ［ウィンドウを最大化や最小化するときにアニメーションで表示する］
   - フェード関連のオプション:
      - ［メニューをフェードまたはスライドして表示する］
      - ［ヒントをフェードまたはスライドで表示する］
      - ［メニュー項目をクリック後にフェード アウトする］
3. ［OK］をクリックして、［コントロール パネル］を閉じます。

Windows 7® を実行している KVM ターゲット サーバを設定するには、以下の手順に従います。

1. マウスの設定を行います。
   a. ［スタート］、［コントロール パネル］、［ハードウェアとサウンド］、［マウス］の順に選択します。

   b. [ポインタ オプション] タブをクリックします。
   c. [速度] グループで、以下の操作を行います。
      - ポインタの速度設定をちょうど中間の速度に設定します。
      - [ポインタの精度を高める] チェック ボックスをオフにします。
      - [OK] をクリックします。
2. アニメーション効果とフェード効果を無効にします。
   a. [コントロール パネル]、[システムとセキュリティ] を選択します。
   b. [システム] を選択し、左側のナビゲーション パネルから [システムの詳細設定] を選択します。[システムのプロパティ] ダイアログ ボックスが表示されます。
   c. [詳細設定] タブをクリックします。
   d. [パフォーマンス] グループの [設定] ボタンをクリックして、[パフォーマンス オプション] ダイアログ ボックスを開きます。
   e. [カスタム] オプションで、以下のチェック ボックスをオフにします。
   - アニメーション関連のオプション:
      - [Windows 内のアニメーション コントロールと要素]
      - [ウィンドウを最大化や最小化するときにアニメーションで表示する]
   - フェード関連のオプション:
      - [メニューをフェードまたはスライドして表示する]
      - [ヒントをフェードまたはスライドで表示する]
      - [メニュー項目をクリック後にフェード アウトする]
3. [OK] をクリックして、[コントロール パネル] を閉じます。

Windows 2000 の設定

▶ Windows 2000® を実行している KVM ターゲット サーバを設定するには

1. マウスの設定を行います。
   a. [スタート]、[コントロール パネル]、[マウス] の順に選択します。
   b. [Motion] (動作) タブをクリックします。
      - アクセラレーションを [なし] に設定します。
      - ポインタの速度設定をちょうど中間の速度に設定します。
      - [OK] (OK) をクリックします。
2. アニメーション効果を無効にします。
   a. [コントロール パネル] の [画面] オプションを選択します。

b. [効果] タブをクリックします。
   - [次のアニメーション効果をメニューとヒントに使用する] オプションをオフにします。
3. [OK] をクリックして、[コントロール パネル] を閉じます。

Linux 設定 (標準マウス モードの場合)

注:以下の設定は、標準マウス モード専用に最適化されています。

Linux® を実行している KVM ターゲット サーバを設定するには、以下の手順に従います (グラフィカル ユーザ インタフェース)。

1. マウスの設定を行います。
   a. Red Hat 5 ユーザの場合は、メイン メニュー、[Preferences] (個人設定)、[Mouse] (マウス) の順に選択します。Red Hat 4 ユーザの場合は、[System] (システム)、[Preferences] (個人設定)、[Mouse] (マウス) の順に選択します。[Mouse Preferences] (マウスの設定) ダイアログ ボックスが表示されます。
   b. [Motion] (モーション) タブをクリックします。
   c. [Speed] (速度) グループ内で、[Acceleration] (加速) スライダを正確に中間に設定します。
   d. [Speed] (速度) グループ内で、[Sensitivity] (感度) を低く設定します。
   e. [Drag & Drop] (ドラッグ & ドロップ) グループ内で、しきい値を小に設定します。
   f. [Mouse Preferences] (マウスの設定) ダイアログ ボックスを閉じます。

   注:これらの手順でうまく設定できない場合は、Linux com コマンドラインの方法で説明されているように、コマンド「xset mouse 1 1」を入力します。

2. 画面解像度を設定します。
   a. メイン メニュー、[System Settings] (システム設定)、[Display] (画面) の順に選択します。[Display Settings] (画面の設定) ダイアログ ボックスが表示されます。
   b. [Settings] (設定) タブから、KSX II でサポートされている解像度を選択します。
   c. [OK] をクリックします。

注:ターゲット サーバに接続すると、ほとんどの Linux グラフィカル環境では、コマンド Ctrl+Alt++ を押すと、XF86Config または /etc/X11/xorg.conf (使用中の X サーバ ディストリビューションに応じて決まります) で有効になっているすべての解像度が順にスクロールされ、ビデオ解像度が変更されます。

注:ビデオの解像度を変更した場合は、そのビデオ設定を有効にするために、ターゲット サーバからログアウトし、再度ログインする必要があります。

SUSE Linux 10.1 の設定

注: SUSE Linux® ログイン プロンプトでマウスを同期しないでください。マウス カーソルを同期するには、ターゲット サーバに接続している必要があります。

▶ マウスを設定するには、以下の手順に従います。

1. **[デスクトップ] メニューの [コントロールセンター] を選択します。[Desktop Preferences] (デスクトップの設定) ダイアログ ボックスが表示されます。**
2. [Mouse] (マウス) をクリックします。[Mouse Preferences] (マウスの設定) ダイアログ ボックスが表示されます。
3. [Motion] (動作) タブを開きます。
4. [Speed] (速度) グループ内で、[Acceleration] (加速) スライダを正確に中間位置に設定します。
5. [Speed] (速度) グループ内で、[Sensitivity] (感度) スライダを低く設定します。
6. [Drag & Drop] (ドラッグ & ドロップ) グループ内で、しきい値スライダを小に設定します。
7. [Close] (閉じる) をクリックします。

▶ ビデオを設定するには、以下の手順に従います。

1. [Desktop Preferences] (デスクトップの設定) の [Graphics Card and Monitor] (グラフィックカードとモニター) を選択します。[Card and Monitor Properties] (カードとモニターのプロパティ) ダイアログ ボックスが表示されます。
2. 解像度と垂直走査周波数に、KSX II でサポートされている値が使用されていることを確認します。詳細は、「**サポートされている画面解像度** 『307p. 』」を参照してください。

   注: ビデオの解像度を変更した場合は、そのビデオ設定を有効にするために、ターゲット サーバからログアウトし、再度ログインする必要があります。

Linux の設定の永続化

注: この手順は、使用している Linux® のバージョンによって少し異なる場合があります。

▶ Linux で設定を永続化するには、以下の手順に従います (プロンプト)。

1. [System] (システム) メニュー、[Preferences] (設定)、[Personal] (個人)、[Sessions] (セッション) の順に選択します。
2. [Session Options] (セッション オプション) タブをクリックします。
3. [Prompt on log off] (ログオフ時にプロンプト) チェックボックスをオンにし、[OK] をクリックします。このオプションにより、ログアウト時に現在のセッションを保存するためのプロンプトが表示されます。
4. ログアウトするときに、ダイアログで [Save current setup] (現在の設定を保存) オプションを選択します。
5. [OK] (OK) をクリックします。

ヒント: ログアウト時にプロンプトが表示されないようにするには、代わりに以下の手順に従います。

▶ Linux で設定を永続化するには、以下の手順に従います (プロンプトなし)。

1. [Desktop] (デスクトップ)、[Control Center] (コントロールセンタ)、[System] (システム)、[Sessions] (セッション) の順にを選択します。
2. [Session Options] (セッション オプション) タブをクリックします。
3. [Prompt on the log off] (ログオフ時にプロンプト) チェックボックスをオフにします。
4. [Automatically save changes to the session] (セッションに対する変更を自動保存) チェックボックスをオンにし、[OK] をクリックします。このオプションにより、ログアウト時に現在のセッションが自動的に保存されます。

UNIX の設定の永続化

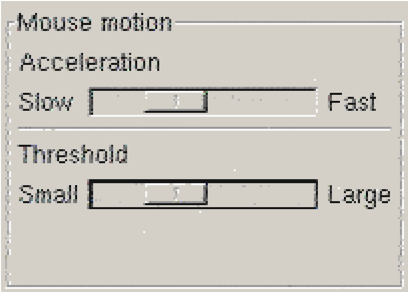
注: これらの手順は、お使いの UNIX® の種類 (例: Solaris™、IBM® AIX™) および特定のバージョンによって少し異なる可能性があります。

1. **[Style Manager] (スタイル マネージャ)、[Startup] (起動) の順に選択します。[Style Manager - Startup] (スタイル マネージャ - 起動) ダイアログ ボックスが表示されます。**
2. [Logout Confirmation] (ログアウトの確認) ダイアログ ボックスで、[On] (オン) オプションを選択します。このオプションにより、ログアウト時に現在のセッションを保存するためのプロンプトが表示されます。

Sun Solaris の設定

▶ Sun™ Solaris™ を実行している KVM ターゲット サーバを設定するには、以下の手順に従います。

1. マウスの加速値を正確に 1 に設定し、しきい値も正確に 1 に設定します。そのためには、以下の操作を行います。
   - グラフィカル ユーザ インタフェースを使用する場合



   - コマンド ラインを使用する場合 *xset mouse a t "a"* は加速 (acceleration)、*"t"* はしきい値 (threshold) を意味します。
2. すべての KVM ターゲット サーバは、KSX II でサポートされているいずれかの表示解像度に設定する必要があります。Sun マシンで一般的にサポートされる解像度を以下に示します。

表示解像度	垂直操作周波数	縦横比
1600 x 1200	60 Hz	4:3
1280 x 1024	60、75、85 Hz	5:4
1152 x 864	75 Hz	4:3
1024 x 768	60、70、75、85 Hz	4:3
800 x 600	56、60、72、75、85 Hz	4:3
720 x 400	85 Hz	9:5
640 x 480	60、72、75、85 Hz	4:3

3. Solaris オペレーティング システムを実行している KVM ターゲット サーバのビデオ出力は、VGA である必要があります (コンポジット Sync ではなく H-and-V sync)。

▶ Sun のビデオ カード出力をコンポジット Sync からデフォルト以外の VGA 出力に変更するには、以下の手順に従います。

1. Stop+A コマンドを発行して、bootprom モードに移行します。
2. 以下のコマンドを発行して、出力解像度を変更します。*setenv output-device screen:r1024x768x70*

3. 次に、`boot` コマンドを実行して、サーバを再起動します。

別の方法として、ラリタンの代理店からビデオ出力アダプタを購入することもできます。

環境	対応するビデオ出力アダプタ
Sun 13W3、コンポジット Sync 出力	APSSUN II Guardian コンバータ
Sun HD15、コンポジット Sync 出力	HD15 から 13W3 への変換用の 1396C コンバータ、およびコンポジット Sync をサポートするための APSSUN II Guardian コンバータ
Sun HD15、独立同期出力	APKMSUN Guardian コンバータ

注: 一部の Sun サーバでは、縁が暗い標準の Sun の背景画面が正確に中央に配置されないことがあります。別の背景を使用するか、画面の左上隅に明るい色のアイコンを配置してください。

マウスの設定

► **マウスを設定するには、以下の手順に従います (Sun Solaris 10.1)。**

1. ランチャーを選択します。アプリケーション マネージャ - デスクトップ コントロールが表示されます。
2. マウス スタイル マネージャを選択します。[Style Manager - Mouse] (スタイル マネージャ - マウス) ダイアログ ボックスが表示されます。
3. 速度のスライダを 1.0 に設定します。
4. しきい値のスライダを 1.0 に設定します。
5. [OK] (OK) をクリックします。

コマンド ラインに対するアクセス

1. 右クリックします。
2. [Tool] (ツール)、[Terminal] (ターミナル) の順に選択します。ターミナル ウィンドウが表示されます (ルートでコマンドを発行することをお勧めします)。

ビデオ設定 (POST)

Sun システムには、2 種類の解像度設定があります。POST の解像度とGUI の解像度です。以下のコマンドをコマンド ラインから実行します。

注: ここでは例として 1024x768x75 を使用しています。お使いの解像度と垂直操作周波数と置き換えてください。

▶ **現在の POST の解像度を確認するには、以下の手順に従います。**

- 次のコマンドを root として実行します。`# eeprom output-device`

▶ **POST の解像度を変更するには、以下の手順に従います。**

1. `# eeprom output-device=screen:r1024x768x75` を実行します。
2. ログアウトするか、コンピュータを再起動します。

ビデオ設定 (GUI)

GUI の解像度は、お使いのビデオ カードに応じたコマンドを使用して確認および設定できます。以下のコマンドをコマンド ラインから実行します。

注: ここでは例として 1024x768x75 を使用しています。お使いの解像度と垂直操作周波数と置き換えてください。

カード	解像度の確認	解像度の変更
32 ビット	# /usr/sbin/pgxconfig -prconf	1. # /usr/sbin/pgxconfig –res 1024x768x75 2. ログアウトするか、コンピュータを再起動します。
64 ビット	# /usr/sbin/m64config –prconf	1. # /usr/sbin/m64config –res 1024x768x75 2. ログアウトするか、コンピュータを再起動します。
32 ビットおよび 64 ビット	# /usr/sbin/fbconfig –prconf	1. # /usr/sbin/fbconfig –res 1024x768x75 2. ログアウトするか、コンピュータを再起動します。

IBM AIX 5.3 の設定

IBM® AIX™ 5.3 を実行している KVM ターゲット サーバを設定するには、以下の手順に従います。

▶ **マウスを設定するには、以下の手順に従います。**

1. ランチャーに移動します。
2. [Style Manager] (スタイル マネージャ) を選択します。
3. [Mouse] (マウス) をクリックします。[Style Manager - Mouse] (スタイル マネージャ - マウス) ダイアログ ボックスが表示されます。
4. スライダを使用して、[Mouse acceleration] (マウスの加速) を 1.0 に設定し、[Threshold] (しきい値) を 1.0 に設定します。
5. [OK] (OK) をクリックします。

▶ **ビデオを設定するには、以下の手順に従います。**

1. ランチャーから、[Application Manager] (アプリケーション マネージャ) を選択します。
2. [System_Admin] を選択します。
3. [Smit]、[Devices] (デバイス)、[Graphic Displays] (グラフィック表示)、[Select the Display Resolution and Refresh Rate] (表示解像度と垂直操作周波数の選択) の順に選択します。
4. お使いのビデオ カードを選択します。
5. [List] (リスト) をクリックします。表示モードの一覧が表示されます。
6. KSX II でサポートされている解像度および垂直走査周波数を選択します。詳細は、「*サポートされている画面解像度* 『*307*p. 』」を参照してください。

注: ビデオの解像度を変更した場合は、そのビデオ設定を有効にするために、ターゲット サーバからログアウトし、再度ログインする必要があります。

Apple Macintosh の設定

Mac® オペレーティング システムが稼動している KVM ターゲット サーバでマウスを正しく同期させるには、ずれないマウス機能が必要です。

ずれないマウス機能を正常に動作させるには、仮想メディア CIM が必要です。サポートされている CIM については、「サポートされているコンピュータ インタフェース モジュール (CIM) の仕様」を参照してください。

KSX II の設置が完了したら、Mac USB プロファイルを設定します。このプロファイルを設定しない場合、OS X でマウスの同期が行われます。

次のいずれかの手順を実行します。

1. Raritan KVM Client から Mac ターゲットに接続します。

2. [USB Profile] (USB プロファイル)、[Other Profiles] (他のプロファイル)、[Mac OS-X (10.4.9 and later)] (Mac OS-X (10.4.9 以降)) の順に選択します。

   または

3. KSX II で、[Device Settings] (デバイス設定) の [Port Configuration] (ポート設定) を選択し、ターゲット名をクリックして [Port] (ポート) ページを開きます。
4. [Select USB Profiles for Port] (ポートの USB プロファイルの選択) セクションを展開します。
5. [Available] (利用可能)ボックスから [Mac OS-X (10.4.9 and later)] (Mac OS-X (10.4.9 以降)) を選択し、[Add] (追加) をクリックして [Selected] (選択) ボックスに追加します。
6. [Selected] (選択) ボックスの [Mac OS-X (10.4.9 and later)] (Mac OS-X (10.4.9 以降)) をクリックします。これにより、選択したプロファイルが [Preferred Profile] (優先プロファイル) ドロップダウンに自動的に追加されます。
7. [Preferred Profile] (優先プロファイル) ドロップダウンから [Mac OS-X (10.4.9 and later)] (Mac OS-X (10.4.9 以降)) を選択し、[Set Active Profile As Preferred Profile] (アクティブ プロファイルを優先プロファイルとして設定) のチェックボックスをオンにします。

[OK] をクリックして適用します。

注: [USB Profile] (USB プロファイル) メニューまたは [Port Configuration] (ポート設定) ページから USB プロファイル [Mac OS-X, version 10.4.9 and later] (MAC OS X (10.4.9 以降)) を選択する必要があります。

ステップ 2: ネットワーク ファイアウォールの設定

Multi-Platform Client を使用してネットワーク ファイアウォールを介して、または [Port Access] (ポート アクセス) ページを介して KSX II にアクセスするには、TCP ポート 5000 または指定した他のポートでの通信を許可するようにファイアウォールを設定する必要があります。

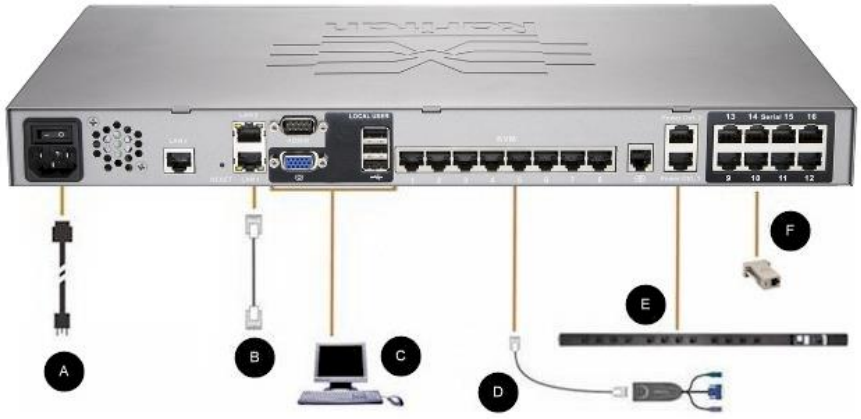
KSX II の機能	ファイアウォールでインバウンド通信を許可する必要があるポート
Web アクセス機能	ポート 443 - HTTPS 通信用の標準 TCP ポート
HTTP リクエストの HTTPS への自動リダイレクト ("https://xxx.xxx.xxx.xxx" の代わりにより一般的な	ポート 80 - HTTP 通信用の標準 TCP ポート

"http://xxx.xxx.xxx.xxx" を使用できるようにする機能)	

別の検出ポートを指定する方法についての詳細は、「*ネットワーク設定*『*147*p. 』」を参照してください。

ステップ 3: 装置の接続

KSX II を、電源、ネットワーク、ローカル PC、KVM ターゲット サーバ、およびシリアル ターゲットに接続します。



A. AC 電源:

▶ 電源を接続するには、以下の手順に従います。

1. 付属の AC 電源コードを KSX II と AC 電源コンセントに接続します。

B. ネットワーク ポート

KSX II は、フェイルオーバ用に 2 つの Ethernet ポートを提供しています (負荷分散用ではない)。デフォルトでは LAN1 のみがアクティブで、自動フェイルオーバは無効になっています。自動フェイルオーバが有効な場合、KSX II の内部ネットワーク インタフェース、またはその接続先のネットワークが使用できなくなると、同じ IP アドレスで LAN2 が利用可能になります。

注: フェイルオーバ ポートは実際にフェイルオーバが発生するまで有効にならないので、フェイル オーバ ポートを監視しないか、フェイルオーバが発生した後にのみ監視するようにすることをお勧めします。

ネットワークを接続するには、以下の手順に従います。

1. (付属の) 標準 Ethernet ケーブルを、「LAN1」のラベルの付いたネットワーク ポートから、Ethernet スイッチ、ハブ、またはルータに接続します。
2. オプションの KSX II Ethernet フェイルオーバ機能を使用するには、以下の手順に従います。
   - 標準 Ethernet ケーブルを、「LAN2」のラベルの付いたネットワーク ポートから、Ethernet スイッチ、ハブ、またはルータに接続します。
   - [Network Configuration] (ネットワーク設定) ページで [Enable Automatic Failover] (自動フェイルオーバを有効にする) をオンにします。

注: 1 つをフェイルオーバ用のポートとして使用する場合のみ、ネットワーク ポートを 2 つ使用してください。

C. ローカル ユーザ ポート (ローカル PC) およびローカル管理ポート

KSX II のローカル アクセス ポートを使用することによって、ラックから KVM ターゲット サーバおよびシリアル デバイスに簡単にアクセスできます。ローカル ポートはインストールおよび設定に必要ですが、それ以降の使用についてはオプションです。ローカル ポートは、管理およびターゲット サーバへのアクセスのための KSX II ローカル コンソール グラフィカル ユーザ インタフェースを提供します。

ローカル ユーザ ポートに接続するには、以下の手順に従います。

- マルチシンク VGA モニタ、キーボード、マウスを、対応するローカル ユーザ ポートに接続します 。

接続	説明
モニタ	標準マルチシンク VGA モニタを

接続	説明
	HD15 (メス) ビデオ ポートに接続します。
キーボード	標準 USB キーボードを USB タイプ A (メス) ポートのいずれかに接続します。
マウス	標準 USB マウスを USB タイプ A (メス) ポートのいずれかに接続します。

ローカル管理ポートを使用して KSX II をワークステーションに直接接続し、シリアル ターゲットを管理したり、HyperTerminal などのターミナル エミュレーション プログラムを使用してシステムを設定したりできます。ローカル管理ポートには、標準のヌル モデム ケーブルを使用する必要があります。

注: ローカルの承認と認証が [None] (なし) に設定されている場合、シリアル管理コンソールにログインするにはユーザ名を入力する必要があります。

D. KVM ターゲット サーバ ポート

KSX II は、標準 UTP ケーブル (Cat5/5e/6) を使用して各ターゲット サーバに接続します。 詳細は、「***仕様*** 『*297*p. 』」を参照してください。

▶ KVM ターゲット サーバを KSX II に接続するには、以下の手順に従います。

1. 適切なコンピュータ インタフェース モジュール (CIM) を使用します。 各オペレーティング システムに対応する CIM についての詳細は、「***サポートされているオペレーティング システムおよび CIM (KVM ターゲット サーバ)*** 『*299*p. 』」を参照してください。
2. お使いの CIM の HD15 ビデオ コネクタを KVM ターゲット サーバのビデオ ポートに接続します。ターゲット サーバのビデオが、サポートされている解像度と垂直走査周波数に設定されていることを確認します。Sun サーバの場合は、ターゲット サーバのビデオ カードがコンポジット Sync ではなく標準 VGA (H-and-V Sync) を出力するように設定されていることも確認してください。
3. お使いの CIM のキーボード/マウス コネクタを、ターゲット サーバの該当するポートに接続します。標準ストレート UTP (Cat5/5e/6) ケーブルを使って、CIM を KSX II デバイスの背面の使用可能なサーバ ポートに接続します。

注: DCIM-USB G2 の背面には小さいスライド型スイッチがあります。PC ベースの USB ターゲット サーバの場合はスイッチを P にします。Sun の USB ターゲット サーバの場合はスイッチを S にします。

変更後のスイッチ位置が有効になるのは、CIM に給電し直した後です。CIM に給電し直すには、ターゲット サーバから USB コネクタをいったん取り外し、数秒経ってから再度取り付けます。

E. ラック PDU (電源タップ)

▶ Dominion PX を KSX II に接続するには、以下の手順に従います。

1. Cat5 ケーブルの一端を Dominion PX の前面にあるシリアル ポートに差し込みます。
2. Cat5 ケーブルのもう一端を、KSX II の背面にある電源制御 1 または電源制御 2 に接続します。
3. AC 電源コードをターゲット サーバと空いているラック PDU コンセントに接続します。
4. ラック PDU を AC 電源に接続します。
5. KSX II デバイスの電源をオンにします。

重要: CC-SG を使用している場合、電源ポート間で切り換えたラック PDU を取り付けるまで電源ポートは非アクティブです。これを完了していない場合、特に 8 および 20 個のコンセントのラック PDU モデルを切り換えた後に、電源コンセントの数が正しく検出されない可能性があります。

図の説明			
A	KSX II	D	PX シリアル ポート
B	KSX II の電源制御 1 または電源制御 2 ポート	1	Cat5 ケーブル
C	PX		

F. シリアル ターゲット ポート

シリアル ターゲットを KSX II に接続するには、適切なシリアル アダプタ付きの Cat5 ケーブルを使用してください。

KSX II を一般的なベンダ/モデルの組み合わせに接続するときに必要な KSX II ハードウェア（アダプタやケーブル）を次の表に示します。

ベンダ	デバイス	コンソール コネクタ	シリアル接続
チェックポイント	ファイアウォール	DB9M	ASCSDB9F アダプタと CAT 5 ケーブル
Cisco	PIX ファイアウォール		
Cisco	Catalyst	RJ-45	CRLVR-15 ロールオーバー ケーブル、または CRLVR-1 アダプタ ケーブルと CAT5 ケーブル このコネクタを持つ KSX II-48 の各モデルのターミナル ポート (RJ-45 コネクタタイプ) を別の KSX II に接続するための CRLVR-1 ケーブル。

ベンダ	デバイス	コンソール コネクタ	シリアル接続
Cisco	ルータ	DB25F	ASCSDB25M アダプタと CAT 5 ケーブル
Hewlett Packard®	UNIX® サーバ	DB9M	ASCSDB9F アダプタと CAT 5 ケーブル
Silicon Graphics	Origin		
Sun™	SPARCStation	DB25F	ASCSDB25M アダプタと CAT 5 ケーブル
Sun	Netra T1	RJ-45	CRLVR-15 ケーブル、または CRLVR-1 アダプタと CAT5 ケーブル
Sun	Cobalt	DB9M	ASCSDB9F アダプタと CAT 5 ケーブル
各種ベンダ	Windows NT®		

一般的に使用されるケーブルやアダプタの一覧については、Raritan の Web サイト (www.raritan.com) のサポート ページを参照してください。

手順 4: KSX II の設定

KSX II デバイスの電源を初めてオンにしたときは、KSX II ローカル コンソールで以下の操作を行う必要があります。

- デフォルト パスワードの変更
- IP アドレスの割り当て
- 日付/時刻の設定 (オプション)
- KVM ターゲット サーバの命名

Web ブラウザを使用して KSX II をリモートで設定できます。ただし、リモート クライアントに適切なバージョンの Java Runtime Environment (JRE) がインストールされている必要があります。

デフォルト パスワードの変更

KSX II の出荷時には、デフォルトのパスワードが設定されています。KSX II を初めて起動したときは、このパスワードを変更する必要があります。

▶ デフォルトのパスワードを変更するには、以下の手順に従います。

1. 本体が起動したら、デフォルトのユーザ名（admin）とパスワード（raritan）を入力します。[ログイン] をクリックします。
2. 古いパスワード（raritan）を入力し、新しいパスワードを入力した後、もう一度新しいパスワードを入力します。パスワードには、最大 64 文字の英数字と特殊文字を使用できます。[適用] をクリックします。[確認] ページで [OK] をクリックします。
3. 注: デフォルトのパスワードは Raritan Multi-Platform Client (MPC) からも変更できます。

注: デフォルトのパスワードは Raritan Multi-Platform Client (MPC) からも変更できます。詳細については、「パスワードの変更」を参照してください。

IP アドレスの割り当て

ここでは、[Network Settings] (ネットワーク設定) ページで IP アドレスを割り当てる方法について説明します。このページのすべてのフィールドおよび操作についての詳細は、「***ネットワーク設定*** 『*147*p. 』」を参照してください。

▶ IP アドレスを割り当てるには、次の手順に従います。

1. [Device Settings] (デバイス設定) の [Network] (ネットワーク) を選択します。[ネットワーク設定] (Network Settings) ページが開きます。
2. KSX II デバイスにわかりやすいデバイス名を指定します。最大 32 文字の英数字と有効な特殊文字を組み合わせて使用できます。スペースは使用できません。
3. [IPv4] (IPv4) セクションで、IPv4 固有の適切なネットワーク設定を入力するか、選択します。
   a. 必要に応じて IP アドレスを入力します。デフォルトの IP アドレスは「192.168.0.192」です。
   b. サブネット マスクを入力します。デフォルトのサブネット マスクは「255.255.255.0」です。
   c. [IP Auto Configuration] (IP 自動設定) ドロップダウンから [None] (なし) を選択した場合は、デフォルトのゲートウェイを入力します。
   d. [IP Auto Configuration] (IP 自動設定) ドロップダウンから [DHCP] (DHCP) を選択した場合は、優先ホスト名を入力します。

e. [IP Auto Configuration] (IP 自動設定) を選択します。次のオプションを使用できます。

- [None] (なし) (静的 IP) – このオプションを選択した場合は、ネットワーク パラメータを手動で指定する必要があります。

  KSX II はインフラストラクチャ デバイスであり、IP アドレスは変更されないので、このオプションが推奨されます。

- [DHCP] (DHCP) – DHCP サーバから一意の IP アドレスとその他のパラメータを取得するために、ネットワークに接続しているコンピュータ (クライアント) によって Dynamic Host Configuration Protocol が使用されます。

  このオプションを選択した場合、ネットワーク パラメータは DHCP サーバによって割り当てられます。DHCP を使用する場合は、[Preferred host name] (優先ホスト名) を入力します (DHCP のみ)。最大 63 文字まで使用できます。

4. IPv6 を使用する場合は、[IPv6] セクションで、適切な IPv6 固有のネットワーク設定を入力するか、選択します。

a. セクション内のフィールドを有効にするには、[IPv6] チェックボックスをオンにします。

b. [Global/Unique IP Address] (グローバル/一意の IP アドレス) を入力します。これは、KSX II に割り当てられる IP アドレスです。

c. [Prefix Length] (固定長) を入力します。これは、IPv6 アドレスで使用されるビット数です。

d. [Gateway IP Address] (ゲートウェイ IP アドレス) を入力します。

e. [Link-Local IP Address] (リンク – ローカル IP アドレス)。このアドレスは、自動的にデバイスに割り当てられます。これは、近隣探索、またはルータが存在しない場合に使用されます。**[Read-Only] (読み取り専用)**

f. [Zone ID]。これは、アドレスが関連付けられているデバイスを識別します。**[Read-Only] (読み取り専用)**

g. [IP Auto Configuration] (IP 自動設定) を選択します。次のオプションを使用できます。

- [None] (設定しない) – 自動 IP 設定を使用せず、IP アドレスを自分で設定する場合は、このオプションを選択します (静的 IP)。推奨されるデフォルトのオプションです。

  [IP auto configuration] (IP 自動設定) で [None] (設定しない) を選択すると、[Network Basic Settings] (ネットワーク基本設定) フィールド ([Global/Unique IP Address] (グローバル/一意の IP アドレス)、[Prefix Length] (固定長)、[Gateway IP Address] (ゲートウェイ IP アドレス)) が有効になり、IP アドレスを手動で設定できるようになります。

- [Router Discovery] (ルータ検出) – このオプションを使えば、グローバルな IPv6 アドレスまたは、ローカルにリンクしたアドレスを大きく超えるユニーク ローカルの IPv6 に自動的に割り当てられます。これはサブネットへの直接接続に限定して適用されます。

5. [DHCP] が選択され、[Obtain DNS Server Address] (DNS サーバ アドレスを取得) が有効になっている場合は、[Obtain DNS Server Address Automatically] (DNS サーバ アドレスを自動的に取得) を選択します。[Obtain DNS Server Address Automatically] (DNS サーバ アドレスを自動的に取得) が選択されると、DHCP サーバが提供する DNS 情報が使用されます。
6. [Use the Following DNS Server Addresses] (次の DNS サーバ アドレスを使用) を選択する場合は、[DHCP] が選択されているかどうかにかかわらず、このセクションに入力されたアドレスが、DNS サーバの接続に使用されます。

   [Use the Following DNS Server Addresses] (次の DNS サーバ アドレスを使用) オプションを選択する場合は、次の情報を入力します。これらのアドレスは、停電によりプライマリ DNS サーバ接続が切断された場合に使用されるプライマリおよびセカンダリ DNS アドレスです。

   a. [Primary DNS Server IP Address] (プライマリ DNS サーバ IP アドレス)
   b. [Secondary DNS Server IP Address] (セカンダリ DNS サーバ IP アドレス)
7. 完了したら [OK] をクリックします。

[Network Settings] (ネットワーク設定) ページのこのセクションの設定についての詳細は、「*LAN インタフェース設定* 『*152*p. 』」を参照してください。

---

*注: 一部の環境では、[LAN Interface Speed & Duplex] (LAN インタフェースの速度と二重化) のデフォルトである [Autodetect] (自動検出) (自動ネゴシエーション) が選択されている場合にネットワーク パラメータが適切に設定されず、ネットワーク上の問題が発生する場合があります。そのような場合は、KSX II の [LAN Interface Speed & Duplex] (LAN インタフェースの速度と二重化) フィールドを [100 Mbps/Full Duplex] (またはネットワークに合ったオプション) に設定することで問題を解決できます。詳細は、**「*ネットワーク設定 『147*p. 』」を参照してください。*

ターゲット サーバの命名

▶ **ターゲット サーバに名前を付けるには、以下の手順に従います。**

1. まだすべてのターゲット サーバを接続していない場合は、接続します。

2. [Device Settings] (デバイス設定) の [Port Configuration] (ポート設定) を選択し、名前を付けるターゲット サーバの [Port Name] (ポート名) をクリックします。
3. サーバの名前を入力します。

   最大 32 文字の英数字と特殊文字で指定します。
4. [OK] をクリックします。

ターゲット名で使用できる有効な特殊文字

ﾎﾄﾗﾖ	説明	ﾎﾄﾗﾖ	説明
!	感嘆符	;	セミコロン
″	二重引用符	=	等号
#	シャープ記号	>	大なり記号
$	ドル記号	?	疑問符
%	パーセント記号	@	アット記号
&	アンパサンド	[	左角かっこ
(	左かっこ	¥	バックスラッシュ
)	右かっこ	]	右角かっこ
*	アスタリスク	^	キャレット
+	プラス記号	_	アンダースコア
,	コンマ	`	低アクセント
-	ダッシュ	{	左中かっこ
.	ピリオド	|	パイプ記号
/	前方スラッシュ	}	右中かっこ
<	小なり記号	~	ティルデ
:	コロン		

Telnet、IP アドレス、または SSH 経由のダイレクト ポート アクセスの構成

このトピックの情報は、シリアル ターゲット向けにダイレクト ポート アクセスを有効にする方法を取り上げたものです。KSX II への KVM/シリアル ポート接続用にダイレクト ポート アクセスを有効にするには、[Device Services] (デバイス サービス) ページで [Enable Direct Port Access via URL] (URL を介したダイレクト ポート アクセスを有効にする) チェックボックスをオンにします。「*URL を経由したダイレクト ポート アクセスの有効化* 『*156*p. 』」を参照してください。

▶ ダイレクト ポート アクセスを設定するには、以下の手順に従います。

1. [Device Settings] (デバイス設定) の [Device Services] (デバイス サービス) を選択します。[Device Service Settings] (デバイス サービス設定) ページが開きます。
2. SSH および Telnet に使用する IP アドレスとポートをシリアル ターゲットの該当するフィールドに入力します。

   3 つすべてのフィールドを空白のままにしておくと、シリアル ターゲットのダイレクト ポート アクセスが無効になります。ダイレクト ポート アクセスを有効にするには、以下のいずれかを実行する必要があります。

   - グローバル Telnet または SSH アクセスを有効にします。
   - 3 つのフィールドのうち少なくとも 1 つのフィールドに、有効な IP アドレスまたは TCP ポートを入力します。

   重要: 複数のフィールドに入力することは推奨されません。

   以下は、Telnet と IP の例です。

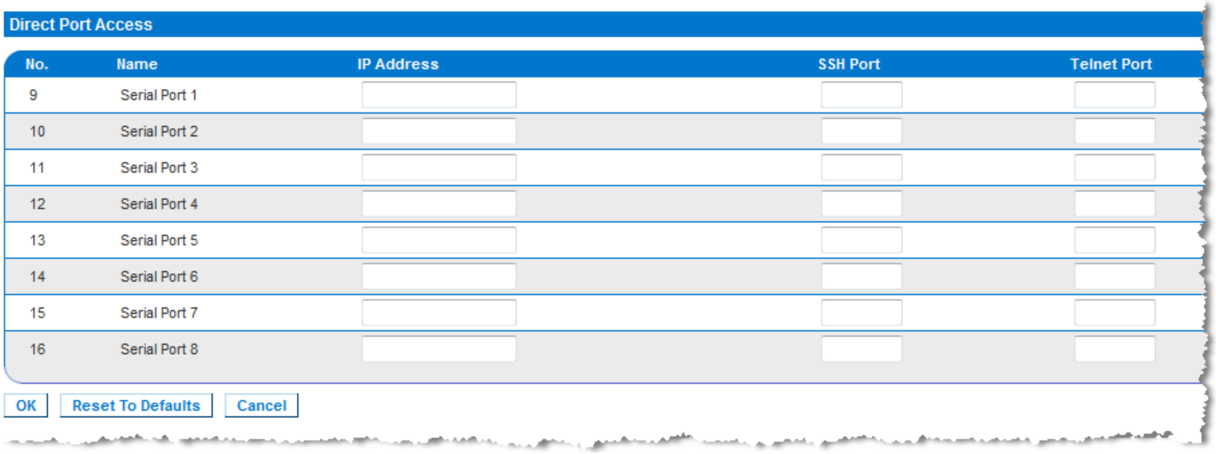
   - IP エイリアス アドレス経由のダイレクト ポート アクセス:

     シリアル ターゲットの IP エイリアス アドレス 192.168.1.59 を設定します。これが完了したら、"telnet 192.168.1.59" を使用して、Telnet 経由でターゲットにアクセスできます。
   - Telnet ポート経由のダイレクト ポート アクセス:

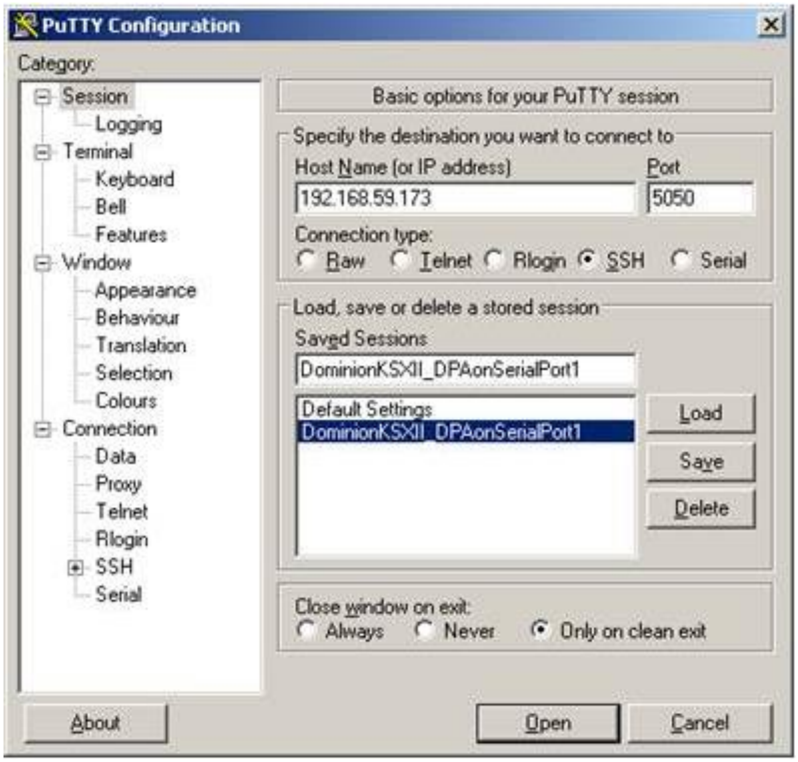
     Telnet TCP ポートを "7770" に設定します。これが完了したら、"telnet <KSX II device IP address> 7770" を使用して、ターゲットにアクセスできます。
   - SSH ポート経由のダイレクト ポート アクセス:

     SSH TCP ポートを "7888" に設定します。これが完了したら、"ssh -l <login> <KSX II device IP address> –p 7888" を使用して、ターゲットにアクセスできます。

3. ［OK］をクリックしてこの情報を保存します。



ダイレクト ポート アクセスを作成したら、PuTTY などのクライアント アプリケーションで接続することができます。次に、ダイレクト ポート アクセス情報が PuTTY に表示される例を示します。クライアント アプリケーションとして使用できるのは、PuTTY だけではありません。ここでは、例示するためにのみ PuTTY を使用しています。



CC-SG ユーザへの注意事項

CC-SG ユーザへの注意事項

KSX II を CC-SG 設定で使用している場合は、インストールを行い、その後、CommandCenter Secure Gateway **のユーザ ガイド**、**管理者ガイド**、**デプロイメント ガイド**のいずれかを参照して作業を続行してください（これらのガイドはラリタンの Web サイト（www.raritan.com）内の「Support」セクションから入手できます）。

注: このヘルプの以降のセクションでは、CC-SG の統合機能なしに KSX II デバイスを展開する作業を中心に説明します。

リモート認証

CC-SG ユーザへの注意事項

CommandCenter Secure Gateway を使用して KSX II を制御している場合、ローカル ポート アクセスを必要とするローカル ユーザを除き、ユーザおよびグループは CC-SG によって認証されます。

CC-SG で KSX II を制御している場合、ローカル ポート ユーザは、KSX II 上で設定されているローカル ユーザ データベースまたはリモート認証サーバ（LDAP/LDAPS または RADIUS）に対して認証され、CC-SG ユーザ データベースに対して認証されません。

CC-SG 認証の詳細については、『CommandCenter Secure Gateway **ユーザ ガイド**』、『CommandCenter Secure Gateway **管理者ガイド**』、または『CommandCenter Secure Gateway **デプロイメント ガイド**』を参照してください。これらは、***Raritan の Web サイト http://www.raritan.com*** の「Support」セクションからダウンロードできます。

サポートされているプロトコル

ユーザ名とパスワードの管理を容易にするため、KSX II には認証要求を外部認証サーバへ転送する機能があります。LDAP/LDAPS と RADIUS の 2 つの外部認証プロトコルがサポートされています。

Microsoft Active Directory についての注意事項

Microsoft® Active Directory® は、LDAP/LDAPS プロトコルをネイティブに使用し、LDAP/LDAPS サーバおよび KSX II の認証元として機能することが可能です。IAS（インタフェース認可サーバ）のコンポーネントを装備している場合、Microsoft Active Directory サーバは、RADIUS 認証元としても機能します。

ユーザ グループおよびユーザを作成する

KSX II にアクセスするためには、初期設定の一環としてユーザ グループおよびユーザを定義する必要があります。

KSX II では、システムによって定義されているデフォルトのユーザ グループを使用して、グループの作成および目的に合った適切な許可の指定を行えるようになります。

KSX II にアクセスするには、ユーザ名とパスワードが必要です。この情報は、KSX II にアクセスしようとしているユーザを認証するために使用されます。 ユーザ グループやユーザの追加方法および編集方法の詳細については、「**ユーザ管理」を参照してください。**

手順 6: キーボード言語の設定 (オプション)

注:英語 (アメリカ)/インターナショナル キーボードを使用している場合は、この手順を実行する必要はありません。

英語 (アメリカ) 以外の言語を使用する場合は、該当する言語のキーボードを設定する必要があります。

また、クライアント マシンおよび KVM ターゲット サーバのキーボード言語を同じにする必要があります。

キーボード レイアウトを変更する方法の詳細については、お使いのオペレーティング システムのマニュアルを参照してください。

キーボード レイアウト コードの変更 (Sun ターゲット)

この手順は、DCIM-SUSB を使用していて、キーボード レイアウトを別の言語に変更する場合に使用します。

► **キーボード レイアウト コードを変更するには、以下の手順に従います (DCIM-SUSB のみ)。**

1. Sun™ ワークステーション上で [テキスト エディタ] ウィンドウを開きます。
2. Num Lock キーが有効であることを確認した後、キーボードの左の Ctrl キーと Del キーを押します。Caps Lock ライトが点滅して、CIM がレイアウト コード変更モードであることを示します。テキスト ウィンドウに、「`Raritan Computer, Inc. Current keyboard layout code = 22h (US5 UNIX)`」と表示されます。
3. 適切なレイアウト コード (たとえば日本語キーボードは *31*) を入力します。
4. Enter キーを押します。
5. デバイスの電源を切った後、再度電源を入れます。DCIM-SUSB がリセット (電源の再投入) されます。

6. 入力した文字が正しく表示されることを確認します。

Ch 3　ターゲット サーバの使用

この章の内容

インタフェース 44
MPC、VKC、および AKC と組み合わせて使用する場合のプロキシ サーバ設定 59
Virtual KVM Client (VKC) 61
Active KVM Client (AKC) 91
Multi-Platform Client (MPC) 94
Raritan Serial Console (RSC) 95

インタフェース

KSX II には、いつでも、どこからでも簡単なアクセスを可能にするいくつかのインタフェースが用意されています。以下の表に、ターゲット サーバのアクセスおよび管理のためにこれらのインタフェースをローカルおよびリモートで使用できるかどうかを示します。

	ローカル		リモート	
ユーザ インタフェース	**[Access] (アクセス)**	**[Admin] (管理)**	**[Access] (アクセス)**	**[Admin] (管理)**
KSX II ローカル コンソール	✓	✓		
KSX II リモート コンソール			✓	✓
Virtual KVM Client (VKC)			✓	
Active KVM Client (AKC)			✓	✓
Multi-Platform Client (MPC)			✓	✓
Raritan Serial Console (RSC)			✓	
コマンド ライン インタフェース (CLI)	✓	✓	✓	✓

ユーザ ガイドの次のセクションでは、以下のインタフェースを使用した KSX II への接続およびターゲット管理の方法について説明します。

- *KSX II ローカル コンソール インタフェース: KSX II デバイス*『*45*p. の"*KSX II ローカル コンソール: KSX II デバイス*"参照 』
- *KSX II リモート コンソール インタフェース* 『*46*p. 』
- *Virtual KVM Client (VKC)* 『*61*p. 』
- *Active KVM Client (AKC)* 『*91*p. 』
- *Multi-Platform Client (MPC)* 『*94*p. 』
- *Raritan Serial Console (RSC)* 『*95*p. 』
- *コマンド ライン インタフェース (CLI)* 『*249*p. 』

KSX II ローカル コンソール: KSX II デバイス

サーバ ラックに設置した KSX II の場合は、KSX II ローカル コンソールを介して、標準 KVM 管理を行います。KSX II ローカル コンソールは接続されたサーバへの直接 KVM (アナログ) 接続を提供し、これにより、サーバのキーボード、マウス、ビデオ ポートに直接接続しているかのように機能することが可能になります。また、KSX II はシリアル ターゲットへのアクセス時にターミナル エミュレーションも提供します。

KSX II ローカル コンソールと KSX II リモート コンソールのグラフィカル ユーザ インタフェースには、多くの類似点があります。相違点については、ヘルプに記載されています。

KSX II リモート コンソール インタフェース

KSX II リモート コンソールは、ブラウザ ベースのグラフィカル ユーザ インタフェースで、このコンソールを通じて、KSX II に接続されている KVM ターゲット サーバおよびシリアル ターゲットにログインして、KSX II をリモート管理できます。

KSX II リモート コンソールは、接続されているターゲット サーバへのデジタル接続を提供します。KSX II リモート コンソールを使用して KVM ターゲット サーバにログインすると、Virtual KVM Client のウィンドウが開きます。

KSX II ローカル コンソールと KSX II リモート コンソールのグラフィカル ユーザ インタフェースには多くの類似点があります。相違点については、ユーザ マニュアルに記載されています。以下のオプションは KSX II リモート コンソールに用意されていますが、KSX II ローカル コンソールには用意されていません。

- 仮想メディア
- [Favorites] (お気に入り)
- [Backup/Restore] (バックアップ/リストア)
- [Firmware Upgrade] (ファームウェアのアップグレード)
- SSL 証明書

注:Internet Explorer® 7 を使用している場合は、ターゲット サーバへの接続時に権限の問題が生じる可能性があります。これを回避するには、以下の手順に従います。

1. Internet Explorer で [ツール] メニューの [インターネット オプション] をクリックして、[インターネット オプション] ダイアログ ボックスを開きます。

2. [インターネット一時ファイル] セクションで [設定] をクリックします。[設定] ダイアログ ボックスが開きます。

3. [保存しているページの新しいバージョンの確認] セクションで [自動的に確認する] を選択します。

4. [OK] をクリックして設定を適用します。

KSX II リモート コンソールの起動

重要: ブラウザの種類を問わず、KSX II リモート コンソールを起動するためには、デバイスの IP アドレスからのポップアップを許可する必要があります。

お使いのブラウザおよびセキュリティの設定により、セキュリティと証明書に関する各種の警告が表示されることがあります。KSX II リモート コンソールを起動するには、これらの警告を承諾する必要があります。

セキュリティと証明書に関する警告メッセージに対して以下のオプションをオンにすることにより、それ以降にログインしたときに表示される警告メッセージを減らすことができます。

- [今後、この警告を表示しない]
- [この発行元からのコンテンツを常に信頼する]

Microsoft .NET® や Java Runtime Environment® がインストールされており、ネットワーク接続機能を備えたワークステーションから KSX II リモート コンソールにログインします。

KSX II リモート コンソールを起動するには、以下の手順に従います。

1. サポートされている Web ブラウザを起動します。
2. 次のどちらかを入力します。
   - URL: *http://IP-ADDRESS*（Java ベースの Virtual KVM Client を使用する場合）

     または

   - *http://IP-ADDRESS/akc*（Microsoft .NET ベースの Active KVM Client の場合）

   IP-ADDRESS は、KSX II に割り当てられた IP アドレスです。

   また、HTTPS を使用するか、管理者によって割り当てられた、KSX II の DNS 名（適用可能な場合）を使用することもできます。
3. 常に、HTTP の IP アドレスから HTTPS の IP アドレスにリダイレクトされます。
4. ユーザ名とパスワードを入力します。初めてログインする場合は、工場出荷時のデフォルト ユーザ名（admin）とパスワード（すべて小文字の raritan）を使用してログインします。デフォルトのパスワードを変更するように求められます。 [Login]（ログイン）をクリックします。

注: デバイスにアクセスする際にセキュリティ同意書を読むことまたはその内容に同意することを、管理者から要求されている場合、ログイン証明書を入力して [Login]（ログイン）をクリックした後にセキュリティ バナーが表示されます。

リモート コンソールを介して利用できる KSX II の機能についての詳細は、「Virtual KVM Client および Active KVM Client (AKC)」を参照してください。

インタフェースおよび画面操作

KSX II インタフェース

KSX II リモート コンソール インタフェースと KSX II ローカル コンソール インタフェースは、デバイス設定および管理、ターゲット サーバのリストおよび選択用に、Web ベース インタフェースを備えています。オプションは複数のタブに配置されています。

正常にログインすると、[ポート アクセス] ページが表示され、すべてのポートについて、そのステータスと可用性が表示されます。このページの 4 つのタブでは、ポート別またはグループ別に表示したり、検索して表示したりできます。列の見出しをクリックすることで、ポート番号、ポート名、ステータス ([Up] (アップ) および [Down] (ダウン))、可用性 ([Idle] (アイドル)、[Connected] (接続済み)、[Busy] (ビジー)、[Unavailable] (使用不可能)、[Connecting] (接続中)) で並べ替えを行うことができます。詳細については、「[Port Access] (ポート アクセス) ページ (リモート コンソール ディスプレイ)」を参照してください。

[Set Scan] (スキャン設定) タブを使用して、KSX II に接続されているターゲットを 32 台までスキャンできます。「ポートのスキャン」を参照してください。

Raritan.

左パネル

KSX II インタフェースの左パネルにある情報は次のとおりです。

一部の情報は、特定の条件に従って、つまり役割や利用する機能などに基づいて表示されます。各情報が表示される条件もこの表に示します。

情報	説明	表示される条件
[Time & Session] (日時およびセッション)	現在のセッションが開始した日時。	常時
ユーザ	ユーザ名。	常時
[State] (状態)	アプリケーションの現在の状態 (アイドルまたはアクティブ)。アイドル状態の場合、セッションがアイドル状態になっている時間が追跡および表示されます。	常時
[Your IP] (あなたの IP アドレス)	KSX II にアクセスする際に使用された IP アドレス。	常時
[Last Login] (最終ログイン日時)	最後にログインした日時。	常時
[Under CC-SG Management] (CC-SG の管理下)	KSX II を管理している CC-SG デバイスの IP アドレス。	KSX II が CC-SG の管理下にある場合。
デバイス情報	使用している KSX II に特有の情報。	常時
[Device Name] (デバイス名)	デバイスに割り当てられている名前。	常時
IP アドレス	KSX II の IP アドレス。IPv6 を有効にすると、IPv6 アドレスもリストされます。	常時
[Firmware] (ファームウェア)	ファームウェアの現在のバージョン。	常時
[Device Model] (デバイス モデル)	KSX II のモデル。	常時

情報	説明	表示される条件
ネットワーク	現在のネットワークに割り当てられている名前。	常時
ポートの状態	KSX II によって現在使用されているポートのステータス。	常時
接続中のユーザー	現在 KSX II に接続している、ユーザ名と IP アドレスによって識別されるユーザ。	常時
[Online Help – User Guide] (オンライン ヘルプ – ユーザ ガイド)	オンライン ヘルプへのリンク。	常時
お気に入りデバイス	「***お気に入りの管理***『*55*p. 』」を参照してください。	常時
[FIPS Mode] (FIPS モード)	FIPS モード: 有効、SSL 証明書: FIPS モード準拠。	FIPS が有効になっている場合。

[Port Access] (ポート アクセス) ページ

KSX II リモート コンソールへのログオンが正常に完了すると、[Port Access] (ポート アクセス) ページに [View by Port] (ポート別に表示) タブが表示されます。このページには、KSX II のすべてのポート、そうしたポートに接続されているターゲット サーバ、ポート グループ、およびブレード シャーシが一覧表示されます。

デフォルトでは、情報はポート番号別に並べられますが、表示されているいずれかの列の見出しをクリックすると、その列で並べ替えて表示されます。タブに一度に表示する行数を増減する場合は、[Rows per Page] (ページ当たりの行数) フィールドに行数を入力し、[Set] (設定) をクリックします。

このページでは、各ポートの次の情報が表示されます。

注: KVM ターゲット サーバへの接続ごとに、新しい Virtual KVM Client ウィンドウが開きます。

また、KSX II で設定されているブレード筐体も表示されます。ブレード サーバは、[Port Access] (ポート アクセス) ページ上の展開可能な階層リストに表示されます。階層のルートはブレード シャーシで、個別のブレードはルートの下にラベルが付けられて表示されます。個別のブレードを表示するには、ルート シャーシの横の展開矢印アイコン ▶ を使用します。

注: ブレード シャーシを階層順に表示するには、ブレード サーバ シャーシにブレード シャーシのサブタイプを設定する必要があります。

[View by Group] (グループ別表示) タブには、ブレード シャーシ、「標準の」ポート グループ、およびデュアル ビデオ ポート グループが表示されます。グループの横の展開矢印アイコン ▶ クリックすると、ポート グループに割り当てられたポートが表示されます。 [View by Search] (検索して表示) タブでは、ポート名で検索できます。検索時にアスタリスク (*) をワイルドカードとして使用できます。また、名前全体で検索することも名前の一部だけで検索することもできます。

▶ [Port Access] (ポート アクセス) ページを使用するには

1. KSX II リモート コンソールで、[Port Access] (ポート アクセス) タブをクリックします。[Port Access] (ポート アクセス) ページが開きます。
2. デフォルトでは、情報はポート番号別に並べられますが、表示されているいずれかの列の見出しをクリックすると、その列で並べ替えて表示されます。
   - [Port Number] (ポート番号) - 1 から KSX II デバイスで使用できるポートの合計数までの番号が振られています。

- [Port Name] (ポート名) – KSX II ポートの名前です。最初は、「Dominion-KSX2-Port#」に設定されていますが、わかりやすい名前に変更できます。[Port Name] (ポート名) のリンクをクリックすると、[Port Action] (ポート アクション) メニューが表示されます。

注: ポート (CIM) 名にアポストロフィ (" ' ") を使用することはできません。

- [Status] (ステータス) – 標準サーバのステータスは [up] (アップ) または [down] (ダウン) のどちらかです。
- [Type] (タイプ) – サーバまたは CIM のタイプです。ブレード シャーシの場合、タイプは、[Blade Chassis] (ブレード シャーシ)、[Blade] (ブレード)、[BladeChassisAdmin] (ブレードシャーシ管理)、および [BladeChassisURL] (ブレードシャーシ URL) です。
- [Availability] (可用性) – 可用性は、[Idle] (アイドル)、[Connected] (接続済み)、[Busy] (ビジー)、または [Unavailable] (使用不可能) のいずれかです。ブレード サーバの場合、そのサーバへの接続が存在する際の可用性は、[shared] (共有) または [exclusive] (排他) です。

3. 必要に応じてビューを切り替えます。切り替えるには、[View by Port] (ポート別に表示) タブ、[View by Group] (グループ別に表示) タブ、または [View by Search] (検索して表示) をクリックします。
4. アクセスするターゲット サーバのポート名をクリックします。[ポート アクション] メニューが表示されます。使用可能なメニュー オプションの詳細については、「*[ポート アクション] メニュー*『*53*p. の *"[Port Action] (ポート アクション) メニュー"*参照 』」を参照してください。
5. [ポート アクション] メニューから、目的のメニュー コマンドを選択します。

▶ 表示順を変更したり同じページにさらにポートを表示したりするには、以下の手順に従います。

1. 並べ替えで基準にする列の見出しをクリックします。その列に基づいて KVM ターゲット サーバのリストが並べ替えられます。

- [1 ページ当たりの行] に、ページに表示するポート数を入力し、[設定] をクリックします。

[Port Action] (ポート アクション) メニュー

[Port Access] (ポート アクセス) リストで [Port Name] (ポート名) をクリックすると、[Port Action] (ポート アクション) メニューが表示されます。

対象のポートに対して適切なメニュー オプションを選択して実行します。[Port Action] (ポート アクション) メニューには、ポートのステータスと可用性に応じて、その時点で利用可能なオプションだけが表示されます。

- [Connect] (接続) – ターゲット サーバへの新しい接続を作成します。

  KSX II リモート コンソールの場合は、新しい *Virtual KVM Client* 『*61*p. の"*Virtual KVM Client (VKC)*"参照 』ページが表示されます。

  KSX II ローカル コンソールの場合は、ローカル ユーザ インタフェースからターゲット サーバに表示が切り替わります。

  ローカル ポートで切り替えを行うためには、KSX II ローカル コンソール インタフェースが表示されている必要があります。

- ローカル ポートからのホット キー切り替えも利用できるようになりました。

注:すべての接続がビジー状態の場合、KSX II リモート コンソールで使用可能なポートに対してこのオプションは使用できません。

- [Switch From] (切り替え元) – 既存の接続から選択したポート (KVM ターゲット サーバ) に切り替えます。
- このメニュー項目は、KVM ターゲットに対してのみ、また Virtual KVM Client が開いている場合にのみ使用できます。

注: KSX II ローカル コンソールでは、このメニュー項目は使用できません。

- [Disconnect] (切断) – このポートを切断し、このターゲット サーバの Virtual KVM Client ページを閉じます。
- このメニュー項目は、ポート ステータスが [up] (アップ) および [connected] (接続済み) であるか、または [up] (アップ) および [busy] (ビジー) であるときにのみ使用できます。

注: KSX II ローカル コンソールでは、このメニュー項目は使用できません。ローカル コンソールで切り替えたターゲットを切断する唯一の方法は、ホットキーを使用することです。

- [Power On] (電源オン) – 関連付けられているコンセントを介してターゲット サーバの電源をオンにします。このオプションは、1 つまたは複数の電源がターゲットに関連付けられているとき、およびこのサービスを操作する許可がユーザーに与えられているときにのみ表示されます。
- [Power Off] (電源オフ) – 関連付けられているコンセントを介してターゲット サーバの電源をオフにします。このオプションは、1 つまたは複数の電源がターゲットに関連付けられているとき、ターゲットの電源がオン (ポート ステータスが [Up] (アップ)) のとき、およびこのサービスを操作する許可がユーザーに与えられているときにのみ表示されます。
- [Power Cycle] (電源の再投入) – 関連付けられているコンセントを介してターゲット サーバの電源をいったんオフにしてから再びオンにします。このオプションは、1 つまたは複数の電源がターゲットに関連付けられているとき、およびこのサービスを操作する許可がユーザーに与えられているときにのみ表示されます。

お気に入りの管理

お気に入り機能を利用すると、よく使用するデバイスにすばやくアクセスできます。

[Port Access] (ポート アクセス) ページの左下隅 (サイドバー) にある [Favorite Devices] (お気に入りデバイス) セクションでは、以下の操作が可能です。

- お気に入りデバイスのリストを作成および管理する。
- よく使用するデバイスにすばやくアクセスする。
- 名前、IP アドレス、または DNS ホスト名別にお気に入りのリストを表示する。
- サブネット上の KSX II デバイスを検出する (ログインの前および後)。
- 検出された KSX II デバイスを、接続されている Dominion デバイスから取得する (ログインの後)。

▶ **お気に入りの KSX II デバイスにアクセスするには、以下の手順に従います。**

- ([Favorite Devices] (お気に入りデバイス) の下に表示されている) デバイス名をクリックします。新しいブラウザが開き、デバイスが表示されます。

▶ **お気に入りを名前順に表示するには、以下の手順に従います。**

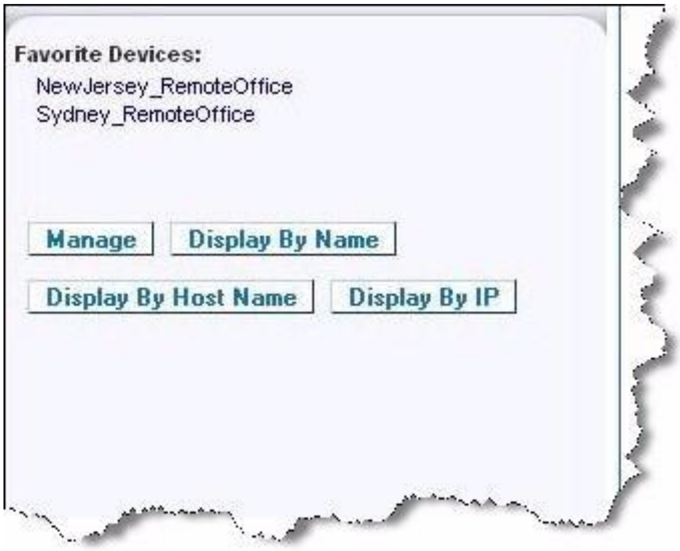
- [Display by Name] (名前順) をクリックします。

▶ **お気に入りを IP アドレス順に表示するには、以下の手順に従います。**

- [Display by IP] (IP 順) をクリックします。

▶ **お気に入りをホスト名順に表示するには、以下の手順に従います。**

- [Display by Host Name] (ホスト名順) をクリックします。



[お気に入りの管理] ページ

▶ **[お気に入りの管理] ページを開くには、以下の手順に従います。**

- 左パネルの［管理］をクリックします。次の内容を含む［お気に入りの管理］ページが表示されます。

メニュー	目的
［お気に入りリスト］	お気に入りデバイスのリストを管理します。
［デバイス検出 － ローカル サブネット］	クライアント PC のローカル サブネット上の Raritan デバイスを検出します。
［デバイス検出 － KSX II サブネット］	KSX II デバイス サブネット上の Raritan デバイスを検出します。
［お気に入りへの新しいデバイスの追加］	お気に入りリストのデバイスを追加、編集、および削除します。

[お気に入りリスト] ページ

［お気に入りリスト］ページでは、お気に入りリストのデバイスを追加、編集、および削除できます。

▶ **[お気に入りリスト] ページを開くには、以下の手順に従います。**

- ［管理］の［お気に入りリスト］を選択します。［お気に入りリスト］ページが開きます。

ローカル サブネット上のデバイスの検出

ローカル サブネット（KSX II リモート コンソールが実行されているサブネット）上のデバイスを検出します。このページから直接これらのデバイスにアクセスしたり、お気に入りのリストにデバイスを追加したりできます。「*[お気に入りリスト] ページ*『57p. 』」を参照してください。

▶ **ローカル サブネット上のデバイスを検出するには、以下の手順に従います。**

1. ［管理］の［デバイス検出 - ローカル サブネット］を選択します。［デバイス検出 - ローカル サブネット］ページが表示されます。
2. 目的の検出ポートを選択します。
   - デフォルトの検出ポートを使用するには、［デフォルト ポート 5000 を使用］チェックボックスをオンにします。
   - 別の検出ポートを使用するには、以下の手順に従います。
   a. ［デフォルト ポート 5000 を使用］チェックボックスをオフにします。
   b. ［検出ポート］フィールドに、ポート番号を入力します。
   c. ［保存］をクリックします。
3. ［更新］をクリックします。ローカル サブネット上のデバイスのリストが更新されます。

▶ **デバイスを [お気に入りリスト] に追加するには、以下の手順に従います。**

1. デバイス名または IP アドレスの横にあるチェックボックスをオンにします。
2. ［追加］をクリックします。

▶ **検出されたデバイスにアクセスするには、以下の手順に従います。**

- 対象のデバイスのデバイス名または IP アドレスをクリックします。新しいブラウザが開き、デバイスが表示されます。

KSX II サブネット上のデバイスの検出

デバイス サブネット（KSX II デバイスの IP アドレスそのもののサブネット）上のデバイスを検出します。このページから直接これらのデバイスにアクセスしたり、お気に入りのリストにデバイスを追加したりできます。「*[お気に入りリスト] ページ* 『*57*p. 』」を参照してください。

この機能を使用すると、複数の KSX II デバイスが相互に作用し合い、自動的にデバイスを検知し構成を拡張します。KSX II リモート コンソールは、KSX II のサブネット内の KSX II デバイスおよびその他の Raritan デバイスを自動的に検出します。

▶ デバイス サブネット上のデバイスを検出するには、以下の手順に従います。

1. [管理] の [デバイス検出 - KSX II サブネット] を選択します。[デバイス検出 - KSX II サブネット] ページが表示されます。
2. [更新] をクリックします。ローカル サブネット上のデバイスのリストが更新されます。

▶ デバイスを [お気に入りリスト] に追加するには、以下の手順に従います。

1. デバイス名または IP アドレスの横にあるチェックボックスをオンにします。
2. [追加] をクリックします。

▶ 検出されたデバイスにアクセスするには、以下の手順に従います。

- 対象のデバイスのデバイス名または IP アドレスをクリックします。新しいブラウザが開き、デバイスが表示されます。

お気に入りの追加、削除、および編集

▶ デバイスを [お気に入りリスト] に追加するには、以下の手順に従います。

1. [管理] の [お気に入りへの新しいデバイスの追加] を選択します。[新しいお気に入りの追加] ページが表示されます。
2. わかりやすい説明を入力します。
3. デバイスの IP アドレス/ホスト名を入力します。
4. 必要に応じて検出ポートを変更します。
5. 製品タイプを選択します。
6. [OK] をクリックします。デバイスがお気に入りのリストに追加されます。

▶ **お気に入りを編集するには、以下の手順に従います。**

1. [お気に入りリスト] ページで、目的の KSX II デバイスの横にあるチェックボックスをオンにします。
2. [編集] をクリックします。[編集] ページが表示されます。
3. 必要に応じてフィールドを更新します。
   - 説明
   - [IP アドレス/ホスト名]: KSX II デバイスの IP アドレスを入力します。
   - [ポート] (必要な場合)
   - [製品タイプ]
4. [OK] をクリックします。

▶ **お気に入りを削除するには、以下の手順に従います。**

重要: お気に入りを削除する場合は注意してください。削除を確認するプロンプトは表示されません。

1. 目的の KSX II デバイスの横にあるチェックボックスをオンにします。
2. [削除] をクリックします。お気に入りのリストからお気に入りが削除されます。

ログアウト

▶ **KSX II を終了するには、以下の操作を行います。**

- ページの右上隅の [Logout] (ログアウト) をクリックします。

注:ログアウトすると、開いているすべての Virtual KVM Client セッションとシリアル クライアント セッションが閉じられます。

MPC、VKC、および AKC と組み合わせて使用する場合のプロキシ サーバ設定

プロキシ サーバを使用する必要がある場合、リモート クライアント PC 上で SOCKS プロキシを設定する必要があります。

注: インストールされているプロキシ サーバが HTTP プロキシ プロトコルにのみ対応している場合は、接続できません。

▶ **SOCKS プロキシを設定するには**

1. クライアント上で [コントロール パネル] の [インターネット オプション] を選択します。

a. [接続] タブで [LAN の設定] をクリックします。[ローカル エリア ネットワーク (LAN) の設定] ダイアログ ボックスが開きます。

b. [LAN にプロキシ サーバを使用する] チェック ボックスをオンにします。

c. [詳細] をクリックします。[プロキシの設定] ダイアログ ボックスが開きます。

d. すべてのプロトコルに対してプロキシ サーバを設定します。重要: [すべてのプロトコルで同じプロキシ サーバを使う] チェック ボックスをオンにしないでください。

注: SOCKS プロキシ用のデフォルト ポート (1080) は、HTTP プロキシ用ポート (3128) とは異なります。

---

2. 各ダイアログ ボックスで [OK] をクリックし、設定内容を適用します。

3. Java™ アプレット用のプロキシを設定するため、[コントロール パネル] の [Java] を選択します。

e. [基本] タブで [ネットワーク設定] をクリックします。[ネットワーク設定] ダイアログ ボックスが開きます。

f. [プロキシ サーバを使用] をクリックします。

g. [詳細] をクリックします。[詳細ネットワーク設定] ダイアログ ボックスが開きます。

h. すべてのプロトコルに対してプロキシ サーバを設定します。重要: [すべてのプロトコルで同じプロキシ サーバを使う] チェック ボックスをオンにしないでください。

注: SOCKS プロキシ用のデフォルト ポート (1080) は、HTTP プロキシ用ポート (3128) とは異なります。

---

4. スタンドアロン MPC を使用している場合は、次の手順も実行する必要があります。

i. テキスト エディタで、MPC ディレクトリにある start.bat ファイルを開きます。

j. コマンド ラインにパラメータを挿入します。このパラメータは、"-classpath" の前に挿入します。挿入するパラメータは、「-DsocksProxyHost=<SOCKS プロキシ IP アドレス> -DsocksProxyPort=<SOCKS プロキシ ポート番号>」です。

挿入後のコマンドは次のようになります。

```
start javaw -Xmn128M -Xmx512M -XX:MaxHeapFreeRatio=70
-XX:MinHeapFreeRatio=50 -Dsun.java2d.noddraw=true
-DsocksProxyHost=192.168.99.99 -DsocksProxyPort=1080
-classpath .¥sdeploy.jar;.¥sFoxtrot.jar;.¥jaws.jar;.¥sMpc.jar
com.raritan.rrc.ui.RRCApplication %1
```

Virtual KVM Client (VKC)

このクライアントは Raritan の各種製品で使用されていることに注意してください。このように、ヘルプのこのセクションには、他の製品への参照が表示される場合があります。

Raritan Virtual KVM Client について

リモート コンソールを使用してターゲット サーバにアクセスすると、Virtual KVM Client (VKC) のウィンドウが開かれます。接続されているターゲット サーバごとに 1 つの Virtual KVM Client ウィンドウが表示されます。これらのウィンドウは、Windows® のタスク バーを使用して開くことができます。

注: 一部の機能 (クライアント起動設定、スマート カードなど) は、LX ではサポートされていません。したがって、LX と併用しても AKC や VKC でサポートされません。

注: KX II-101-V2 のみ、一度に 1 台のターゲットへの接続をサポートしています。

Virtual KVM Client ウィンドウは、お使いのコンピュータのデスクトップ上で最小化、最大化、および移動できます。

注: HTML ブラウザ表示を更新すると Virtual KVM Client 接続が切断されてしまうので注意してください。

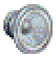
注: Firefox 3.0.3 を使用している場合は、アプリケーションの起動で問題が発生することがあります。この場合は、ブラウザのキャッシュをクリアして、アプリケーションを再起動してください。

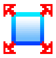
KVM ターゲット サーバへの接続

▶ KVM ターゲット サーバに接続するには、以下の手順に従います。

1. KSX II リモート コンソールで、[Port Access] (ポート アクセス) タブをクリックします。[Port Access] (ポート アクセス) ページが開きます。
2. アクセスしたいターゲット サーバのポート名をクリックします。[Port Action] (ポート アクション) メニューが表示されます。
3. [Connect] (接続) をクリックします。Virtual KVM Client ウィンドウが開き、そのポートに接続されているターゲット サーバが表示されます。

ツール バーのボタンおよびステータス バーのアイコン

ボタン	ボタン名	説明
	[Connection Properties] (接続プロパティ)	帯域幅のオプションを（接続スピード、色深度など）を手動で調節するための［Modify Connection Properties］(接続プロパティの変更）ダイアログ ボックスを開きます。
	[Video Settings] (ビデオ設定)	ビデオ変換パラメータを手動で調節するための［ビデオ設定］ダイアログ ボックスを開きます。
	[Color Calibration] (色調整)	色設定を調節し、余分な色ノイズを低減します。 [Video] (ビデオ) の［Color Calibrate］(色調整) を選択した場合と同じです。 *注: KX II-101-V2 では使用できません。*
	[Target Screenshot] (ターゲット スクリーンショット)	クリックすると、ターゲット サーバのスクリーンショットを取得して、それを選択したファイルに保存します。
	音声	クライアント PC に接続されている音声デバイスのリストから選択するためのダイアログ ボックスを開きます。 音声デバイスがターゲットに接続されたら、デバイスを選択して切断します。 *注: この機能は、KX II 2.4.0 (以降) で使用できます。* *注: この機能は LX ではサポートされていません。*
	[Synchronize Mouse] (マウスの同期)	デュアルマウス モードで、マウス ポインタとターゲット サーバのマウス ポインタを同期させます。 注: ずれないマウス モードが選択されている場合は、使用できません。
	[Refresh Screen] (画面の更新)	ビデオ画面を強制的に更新します。
	[Auto-sense	ビデオ設定を強制的に更新します（解像度、垂直

ボタン	ボタン名	説明
	Video Settings] (ビデオ設定の自動検出)	走査周波数)。
	スマート カード	クライアント PC に接続されているスマート カード リーダーのリストから選択するためのダイアログ ボックスを開きます。 *注: この機能は、KSX II 2.3.0 (以降) および KX II 2.1.10 (以降) で提供されます。* *注: この機能は LX ではサポートされていません。*
	[Send Ctrl+Alt+Del] (Ctrl+Alt+Del の送信)	ターゲット サーバに Ctrl+Alt+Del のキー操作を送信します。
	[Single Cursor Mode] (シングル カーソル モード)	ローカルのマウス ポインタを画面に表示しない「シングル カーソルモード」になります。 このモードを終了するには、Ctrl+Alt+O キーを押します。 *注: KX II-101-V2 では使用できません。*
	[Full Screen Mode] (全画面モード)	ターゲット サーバのデスクトップを表示する画面を最大化します。
	[Scaling] (拡大、縮小)	ターゲットのビデオ サイズを拡大、縮小して、スクロール バーを使用せずにターゲット サーバ ウィンドウの内容をすべて表示できるようにします。

アイコン	アイコン名	説明
	スピーカー	クライアント ウィンドウの下部のステータスバーにあります。 緑色の波が点滅している場合は、音声再生セッションがストリーム配信されていることを示しています。 セッションがミュートされると、黒色のスピーカー アイコンが表示されます。 音声が接続されていない場合、このアイコンはグレーで表示されます。 *注: 音声は、KX II 2.4.0 (以降) でサポートされています。*
	マイク	クライアント ウィンドウの下部のステータスバーにあります。 赤色の波が点滅している場合は、音声キャプチャセッションが現在進行中であることを示しています。 セッションが進行中の場合は、再生セッションがストリーム配信されていることを示すスピーカー アイコンも表示されます。 セッションがミュートされると、黒色のマイク アイコンが表示されます。 音声が接続されていない場合、マイク アイコンはグレーで表示されます。 *注: 音声は、KX II 2.5.0 (以降) でサポートされています。*

KVM ターゲット サーバの切り替え

KSX II では、複数の KVM ターゲット サーバにアクセスできます。KSX II は、ターゲット サーバを切り替える機能を備えています。

注: この機能は、KSX II リモート コンソールでのみ使用できます。

▶ KVM ターゲット サーバを切り替えるには、以下の手順に従います。

1. ターゲット サーバを使用しているときに、KSX II の [ポート アクセス] ページを開きます。

2. アクセスするターゲットの［ポート名］をクリックします。［ポート アクション］メニューが表示されます。
3. ［ポート アクション］メニューの［切り替え元］を選択します。選択した新しいターゲット サーバが表示されます。

ターゲット サーバの電源管理

注: これらの機能は、電源の関連付けを行っている場合にのみ使用できます。

▶ KVM ターゲット サーバの電源を再投入するには、以下の手順に従います。

1. KSX II リモート コンソールで、[Port Access]（ポート アクセス）タブをクリックします。[Port Access]（ポート アクセス）ページが開きます。
2. 適切なターゲット サーバのポート名をクリックします。[Port Action]（ポート アクション）メニューが表示されます。
3. [Power Cycle]（電源の再投入）を選択します。確認メッセージが表示されます。

▶ ターゲット サーバの電源をオンにするには、以下の手順に従います

1. KSX II リモート コンソールで、[Port Access]（ポート アクセス）タブをクリックします。[Port Access]（ポート アクセス）ページが開きます。
2. 適切なターゲット サーバのポート名をクリックします。[Port Action]（ポート アクション）メニューが表示されます。
3. [Power On]（電源オン）を選択します。確認メッセージが表示されます。

▶ ターゲット サーバの電源をオフにするには、以下の手順に従います

1. KSX II リモート コンソールで、[Port Access]（ポート アクセス）タブをクリックします。[Port Access]（ポート アクセス）ページが開きます。
2. 適切なターゲット サーバのポート名をクリックします。[Port Action]（ポート アクション）メニューが表示されます。
3. [Power Off]（電源オフ）を選択します。確認メッセージが表示されます。

KVM ターゲット サーバの切断

注: KSX II ローカル コンソールでは、この項目は使用できません。ローカル コンソールで切り替えたターゲットを切断する唯一の方法は、ホットキーを使用することです。

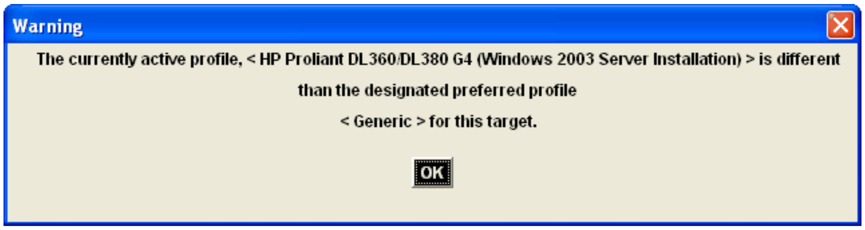
ターゲット サーバを切断するには、以下の手順に従います。

1. [Port Access] (ポート アクセス) ページで、切断するターゲットのポート名をクリックし、表示される [Port Action] (ポート アクション) メニューの [Disconnect] (切断)をクリックします。

ヒント: Virtual KVM メニューの [Connection] (接続) の [Exit] (終了) を選択することによっても Virtual KVM Client ウィンドウを閉じることができます。

USB プロファイルの選択

KVM ターゲット サーバに初めて接続する場合は、「***KVM ターゲット サーバへの接続***『*61*p. 』」で説明されているように、ポートの優先 USB プロファイルが自動的に使用されます。前に別のプロファイルを使用してターゲット サーバに接続したことがある場合は、最後に接続したときの USB プロファイルが使用されます。優先プロファイル以外のプロファイルが使用される場合は、次のような警告で通知されます。



ターゲット サーバに接続した後、必要に応じて USB プロファイルを変更できます。デフォルトでは、VKC の [USB Profile] (USB プロファイル) メニューの下に表示されるプロファイルが、最もよく使用されているプロファイルです。これらのプロファイルは、接続されるターゲット サーバで使用されるものとして操作要件に基づいて管理者があらかじめ選択しています。ただし、すべてのプロファイルは、[USB Profile] (USB プロファイル) メニューの [Other Profile] (他のプロファイル) オプションを使用して選択できます。

USB プロファイルを選択するには、以下の手順に従います。

1. 「***KVM ターゲット サーバへの接続***『*61*p. 』」の説明にしたがって、KVM ターゲット サーバに接続します。
2. VKC で、[USB Profile] (USB プロファイル) メニューから USB プロファイルを選択します。

プロファイルの名前は、それが使用されるオペレーティング システムまたはサーバを示しています。USB プロファイルについての詳細は、「*USB プロファイル* 『*115*p. 』」を参照してください。

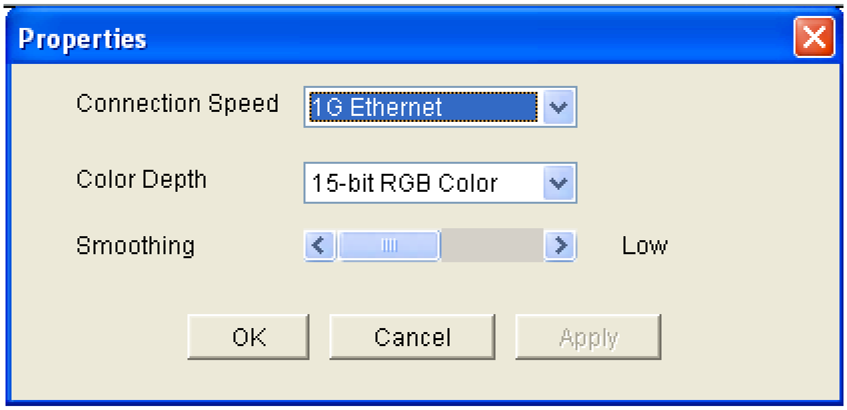
[Connection Properties] (接続プロパティ)

動的ビデオ圧縮アルゴリズムは、さまざまな帯域幅条件で KVM コンソールの使用を可能にします。デバイスの KVM 出力は、LAN 経由だけでなく WAN 経由でも使用できるように最適化されます。さらに、色深度を制御してビデオ出力を制限できるため、さまざまな帯域幅でビデオ画質とシステム応答性のバランスを最適に維持することができます。

[Properties] (プロパティ) ダイアログ ボックスのパラメータは、さまざまな動作環境の要件に合わせて最適に設定できます。 接続プロパティは、一度設定して保存すると、それ以降の第 2 世代デバイスへの接続に使用されます。

▶ 接続プロパティを設定するには、以下の手順に従います。

1. [Connection] (接続) の [Properties] (プロパティ) を選択するか、ツールバーの [Connection Properties] (接続プロパティ) ボタン をクリックします。[Properties] (プロパティ) ダイアログ ボックスが表示されます。



注:KX II-101 は 1G Ethernet をサポートしていません。

2. ドロップダウン リストから接続スピードを選択します。デバイスでは、使用可能な帯域幅を自動的に検出できるため、帯域幅利用は制限されません。ただし、帯域幅の制限に応じて帯域幅利用を調整することもできます。
   - 自動
   - [1G Ethernet] (1G Ethernet)
   - [100 Mb Ethernet] (10 Mbps Ethernet)
   - [10 Mb Ethernet] (10 Mbps Ethernet)
   - [1.5 Mb (MAX DSL/T1)] (1.5 Mbps (最高速 DSL/T1))

- [1 Mb (Fast DSL/T1)] (1 Mbps (高速 DSL/T1))
- [512 Kb (Medium DSL/T1)] (512 Kbps (中速 DSL/T1))
- [384 Kb (Slow DSL/T1)] (384 Kbps (低速 DSL/T1))
- [256 Kb (Cable)] (256 Kbps (ケーブル))
- [128 Kb (Dual ISDN)] (128 Kbps (デュアル ISDN))
- [56 kb (ISP Modem)] (56 Kbps (ISP モデム))
- [33 kb (Fast Modem)] (33 Kbps (高速モデム))
- [24 kb (Slow Modem)] (24 Kbps (低速モデム))

これらの設定は、実際の速度ではなく特定の条件に対して最適化されています。クライアントおよびサーバは、現在のネットワーク速度やエンコード設定に関係なく、常に最高速度でネットワークにビデオを配信しようとします。ただし、システムの応答性が最も高くなるのは、設定が実際の環境と一致するときだけです。

3. ドロップダウン リストから色深度を選択します。デバイスでは、リモート ユーザに送信される色深度を動的に調整することで、さまざまな帯域幅で最適な使いやすさを実現します。
   - [15-bit RGB Color] (8 ビット RGB カラー)
   - [8-bit RGB Color] (8 ビット RGB カラー)
   - [4-bit Color] (4 ビット カラー)
   - [4-bit Gray] (2 ビット グレー)
   - [3-bit Gray] (2 ビット グレー)
   - [2-bit Gray] (2 ビット グレー)
   - [Black and White] (モノクロ)

重要: 多くの管理タスク (サーバの監視、再設定等) において、最新のビデオ グラフィック カードのほとんどで利用できる 24 ビットまたは 32 ビットのフルカラー表示は必要ありません。このような高い色深度を送信すると、ネットワークの帯域幅を浪費することになります。

4. スライダを使用して、スムージングのレベルを指定します (15 ビット カラー モードのみ)。ここで設定したスムージングのレベルにより、色がわずかに異なる画面領域をできるだけ滑らかな単色の組み合わせにするかが決まります。スムージングにより、表示されるビデオ ノイズを軽減することで、対象ビデオの画質が向上します。
5. [OK] をクリックして、これらのプロパティを保存します。

接続情報

▶ **Virtual KVM Client 接続に関する情報を取得するには、以下の手順に従います。**

- [Connection] (接続) の [Info...] (情報...) を選択します。[Connection Info] (接続情報) ウィンドウが開きます。

現在の接続に関する以下の情報が表示されます。

- [Device Name] (デバイス名) – デバイスの名前です。
- [IP Address] (IP アドレス) – デバイスの IP アドレスです。
- [Port] (ポート) – ターゲット デバイスへのアクセスに使用される KVM 通信 TCP/IP ポートです。
- [Data In/Second] (データ入力/秒) – 入力データ レートです。
- [Data Out/Second] (データ出力/秒) – 出力データ レートです。
- [Connect Time] (接続時間) – 接続時間です。
- [FPS] (FPS) – ビデオで送信される毎秒フレーム数です。
- [Horizontal Resolution] (水平解像度) – 水平方向の画面解像度です。
- [Vertical Resolution] (垂直解像度) – 垂直方向の画面解像度です。
- [Refresh Rate] (垂直走査周波数) – 画面の更新頻度を表します。
- [Protocol Version] (プロトコル バージョン) – RFB プロトコル バージョンです。

▶ **この情報をコピーするには、以下の手順に従います。**

- [Copy to Clipboard] (クリップボードにコピー) をクリックします。これにより、任意のプログラムにこの情報を貼り付けることができます。

キーボードのオプション

[Keyboard Macros] (キーボード マクロ)

キーボード マクロを利用することで、ターゲット サーバに対するキー入力が確実にターゲット サーバに送信され、ターゲット サーバのみで解釈されます。キーボード マクロを利用しない場合、Virtual KVM Client が実行されているコンピュータ（クライアント PC）によって解釈される可能性があります。

マクロはクライアント PC に保存され、その PC 専用になります。したがって、別の PC を使用したときは、作成したマクロを使用できません。さらに、キーボード マクロはコンピュータ単位で管理されるので、あるユーザが使用している PC に別のユーザが自分の名前でログインした場合でも、1 人目のユーザが作成したマクロが 2 人目のユーザに対して表示されます。

Virtual KVM Client 内で作成したキーボード マクロは Multi-Platform Client (MPC) で使用でき、またその逆も可能です。ただし、Active KVM Client (AKC) で作成したキーボード マクロは、VKC または MPC で使用できません。また、その逆でも使用できません。

注:KX II-101 は AKC をサポートしていません。

キーボード マクロの作成

▶ マクロを作成するには、以下の手順に従います。

1. [Keyboard] (キーボード) の [Keyboard Macros] (キーボード マクロ) をクリックします。[Keyboard Macros] (キーボード マクロ) ダイアログ ボックスが表示されます。
2. [Add] (追加) をクリックします。[Add Keyboard Macro] (キーボード マクロの追加) ダイアログ ボックスが表示されます。
3. [Keyboard Macro Name] (キーボード マクロ名) フィールドにマクロの名前を入力します。この名前は、マクロが作成された後に [Keyboard] (キーボード) メニューに表示されます。
4. [Hot-Key Combination] (ホットキーの組み合わせ) フィールドで、ドロップダウン リストからキー操作の組み合わせを選択します。これにより、定義済みのキー入力を使用してマクロを実行できます。<オプション>

5. [Keys to Press] (押すキー) ドロップダウン リストで、コマンドの実行に使用されるキー操作のエミュレート用のキーを選択します。押される順にキーを選択します。各キーの選択後に、[Add Key] (キーの追加) を選択します。キーを選択するごとに、[Macro Sequence] (マクロ シーケンス) フィールドに表示されます。また、1 つ選択するごとに、その [Release Key] (キーのリリース) コマンドが自動的に追加されます。

   たとえば、左 Ctrl +Esc を選択して、ウィンドウを閉じるマクロを作成します。これは、[Macro Sequence] (マクロ シーケンス) ボックスに以下のように表示されます。

   [Press Left Alt] (左 Alt の押下)

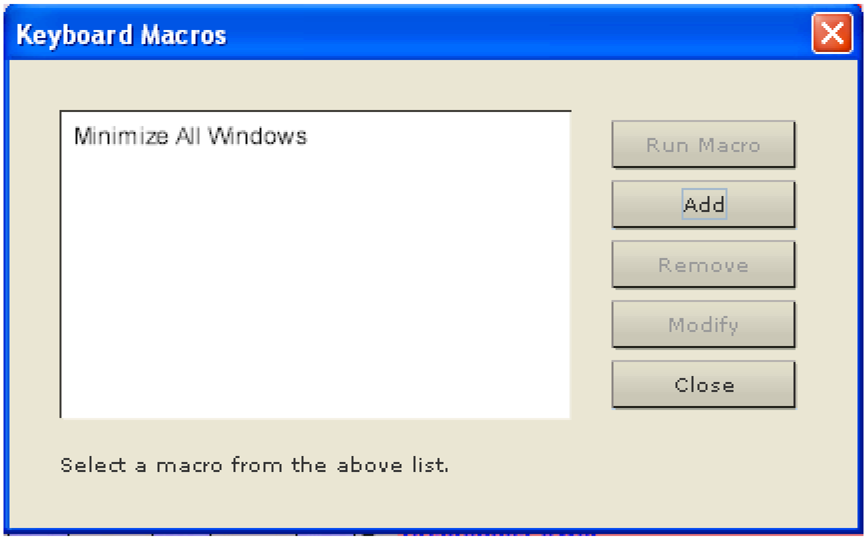
   [Press F4] (F4 の押下)

   [Release F4] (F4 のリリース)

   [Release Left Alt] (左 Alt のリリース)

6. [Macro Sequence] (マクロ シーケンス) フィールドで、マクロ シーケンスが正しく定義されていることを確認します。
   a. キー操作の 1 つの手順を削除するには、手順を選択して [Remove] (削除) をクリックします。
   b. キー操作の手順の順番を変更するには、手順をクリックし、必要に応じて上/下の矢印ボタンをクリックして順序を変更します。
7. [OK] をクリックしてマクロを保存します。[クリア] をクリックすると、すべてのフィールドがクリアされ、最初の状態に戻ります。[OK] をクリックすると [Keyboard Macros] (キーボード マクロ) ウィンドウが表示され、新しいキーボード マクロのリストが表示されます。

8. [Close] (閉じる) をクリックして [Keyboard Macro] (キーボード マクロ) ダイアログ ボックスを閉じます。マクロがアプリケーションの[Keyboard] (キーボード) メニューに表示されます。メニューの新しいマクロを選択して実行するか、マクロに割り当てたキー入力を使用します。



▶ マクロの [Send Text to Target] (テキストをターゲットに送信) 機能を使用するには、以下の手順に従います。

1. [Keyboard] (キーボード) の [Send Text to Target] (テキストをターゲットに送信) をクリックします。[Send Text to Target] (テキストをターゲットに送信) ダイアログ ボックスが表示されます。
2. ターゲットに送信するテキストを入力します。

注:[Send Text to Target] (テキストをターゲットに送信) 機能では、英語以外の文字はサポートされていません。

---

3. ターゲットでアメリカ英語/国際キーボード レイアウトを使用する場合は、[Target system is set to the US/International keyboard layout] (ターゲット システムはアメリカ英語/国際キーボード レイアウトに設定されています) チェックボックスをオンにします。
4. [OK] をクリックします。

キーボード マクロの実行

作成したキーボード マクロは、割り当てたキーボード マクロを使用するか、[Keyboard] (キーボード) メニューからそれを選択して起動します。

メニュー バーからのマクロの実行

マクロを作成すると、そのマクロが [Keyboard] (キーボード) メニューに表示されます。キーボード マクロを実行するには、[Keyboard] (キーボード) メニューでそれをクリックします。

キー操作の組み合わせを使用したマクロの実行

マクロの作成時にキー操作の組み合わせを割り当てた場合は、割り当てたキー入力を押すことでマクロを実行できます。たとえば、Ctrl+Alt+0 キーを同時に押すと、Windows ターゲット サーバの全ウィンドウが最小化されます。

キーボード マクロの変更および削除

▶ **マクロを変更するには、以下の手順に従います。**

1. [Keyboard] (キーボード) の [Keyboard Macros] (キーボード マクロ) を選択します。[Keyboard Macros] (キーボード マクロ) ダイアログ ボックスが表示されます。
2. マクロのリストから目的のマクロを選択します。
3. [Modify] (変更) をクリックします。[Add/Edit Keyboard Macro] (キーボード マクロの追加/編集) ダイアログ ボックスが表示されます。
4. 必要な変更を加えます。
5. [OK] (OK) をクリックします。

▶ **マクロを削除するには、以下の手順に従います。**

1. [Keyboard] (キーボード) の [Keyboard Macros] (キーボード マクロ) を選択します。[Keyboard Macros] (キーボード マクロ) ダイアログ ボックスが表示されます。
2. マクロのリストから目的のマクロを選択します。
3. [Remove] (削除) をクリックします。マクロが削除されます。

ブレード シャーシの切り替えキー シーケンスと一致するホットキーの組み合わせは、それらのシャーシ内のブレードには送信されません。

CIM キーボード/マウス オプションの設定

▶ **DCIM-USBG2 の設定メニューにアクセスするには、以下の手順に従います。**

1. Windows® のメモ帳などのウィンドウにマウス ポインタを置きます。

2. [Set CIM Keyboard/Mouse options] (CIM キーボード/マウス オプションを設定する）を選択します。この操作は、左 Ctrl + Num Lock キーをターゲットに送信することと同じです。CIM セットアップ メニュー オプションが表示されます。
3. 言語とマウスを設定します。
4. メニューを終了し、通常の CIM 機能に戻ります。

ビデオのプロパティ

画面を更新する

[Refresh Screen] (画面の更新）コマンドを使用すると、ビデオ画面が更新されます。ビデオの設定を自動的に更新する方法はいくつかあります。

- [Refresh Screen] (画面の更新）コマンドを使用すると、ビデオ画面が更新されます。
- [Auto-sense Video Settings] (ビデオ設定の自動検出）コマンドを使用すると、ターゲット サーバのビデオ設定が自動的に検出されます。
- [Calibrate Color] (色調整）コマンドを使用すると、ビデオの表示色が調整されます。

これに加え、[Video Settings] (ビデオ設定）コマンドを使用すると、手動で設定を調整できます。

▶ ビデオ設定を更新するには、次のいずれかの手順に従います。

- [Video] (ビデオ）の [Refresh Screen] (画面の更新）を選択するか、ツールバーの [Refresh Screen] (画面の更新）ボタン をクリックします。

[Auto-sense Video Settings] (ビデオ設定の自動検出)

[Auto-sense Video Settings] (ビデオ設定の自動検出）コマンドを使用すると、ビデオ設定（解像度、垂直走査周波数）が再検出され、ビデオ画面が再描画されます。

▶ ビデオ設定を自動的に検出するには、以下の手順に従います。

- [Video] (ビデオ）の [Auto-sense Video Settings] (ビデオ設定の自動検出）を選択するか、ツールバーの [Auto-sense Video Settings] (ビデオ設定の自動検出）ボタン をクリックします。

  調整が行われていることを示すメッセージが表示されます。

色の調整

[Calibrate Color] (色調整) コマンドは、送信されたビデオ画像の色レベル (色相、輝度、彩度) を最適化するために使用します。色設定は、ターゲット サーバごとに適用されます。

注: [Calibrate Color] (色調整) コマンドは、現在の接続のみに適用されます。

▶ **色を調整するには、以下の手順に従います。**

- [Video] (ビデオ) の [Calibrate Color] (色調整) を選択するか、ツールバーの [Calibrate Color] (色調整) ボタン をクリックします。ターゲット デバイス画面の色が調整されます。

ビデオ設定の調整

[Video Settings] (ビデオ設定) コマンドを使用すると、ビデオ設定を手動で調整できます。

▶ **ビデオ設定を変更するには、以下の手順に従います。**

1. [Video] (ビデオ)、[Video Settings] (ビデオ設定) を選択して、[Video Settings] (ビデオ設定) ダイアログ ボックスを開きます。
2. 必要に応じて、以下の設定を調整します。設定を調整すると、その効果が即座に表示に反映されます。
   a. [PLL Settings] (PLL 設定)

      [Clock] (クロック) – ビデオ画面上にビデオ ピクセルが表示される速度を制御します。クロック設定値を変更すると、ビデオ画像が水平方向に伸縮します。設定値は奇数を推奨します。通常は自動検出機能によって適切に設定されるため、ほとんどの環境ではこの設定を変更する必要はありません。

      [Phase] (位相) – 位相の値の範囲は 0 ～ 31 です。これより大きな値は反復されます。アクティブなターゲット サーバ用に最適なビデオ画像が得られる位相の位置で停止してください。
   b. [Brightness] (明るさ): この設定は、ターゲット サーバの画面表示の輝度を調整するために使用します。
   c. [Brightness Red] (赤輝度) – ターゲット サーバの画面に表示される赤の信号の輝度を制御します。
   d. [Brightness Green] (緑輝度) – 緑の信号の輝度を制御します。
   e. [Brightness Blue] (青輝度) – 青の信号の輝度を制御します。
   f. [Contrast Red] (赤コントラスト) – 赤の信号のコントラストを制御します。

g. [Contrast Green]（緑コントラスト）－ 緑の信号のコントラストを制御します。

h. [Contrast Blue]（青コントラスト）－ 青の信号のコントラストを制御します。

ビデオ画像が大幅にぼやけている場合、設定でクロックと位相を調節することで、アクティブなターゲット サーバの画像を改善します。

警告: クロック設定と位相設定を変更する際には、注意が必要です。ビデオ画像が消えたり歪んだりする可能性があるだけでなく、元の状態に戻せなくなることがあります。変更を加える前に、ラリタン テクニカル サポートにお問い合わせください。

---

i. [Horizontal Offset]（水平オフセット）－ ターゲット サーバの画面がモニタに表示されるときの水平位置を制御します。

j. [Vertical Offset]（垂直オフセット）－ ターゲット サーバの画面がモニタに表示されるときの垂直位置を制御します。

3. [Automatic Color Calibration]（自動色調節）を選択して、この機能を有効にします。

4. ビデオ検出モードを選択します。

   - [Best possible video mode]（最適ビデオ モード）

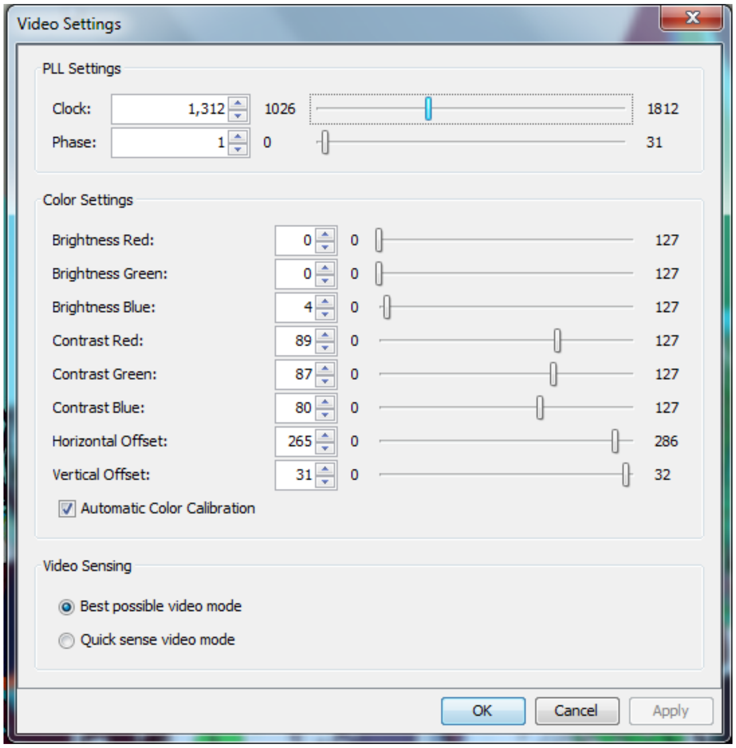
   ターゲットやターゲットの解像度が変更されたときに、すべての自動検出処理が実行されます。このオプションを選択すると、最適な画像品質になるようにビデオが調整されます。

   - [Quick sense video mode]（クイック検出ビデオ モード）

   このオプションを使用すると、クイック ビデオ自動検出が使用され、ターゲットのビデオがより早く表示されます。このオプションは、再起動直後のターゲット サーバの BIOS 設定を入力するときに特に有効です。

5. 設定を適用してダイアログ ボックスを閉じるには、[OK] をクリックします。ダイアログ ボックスを閉じずに設定を適用するには、[Apply]（適用）をクリックします。

注: 一部の Sun サーバでは、ある種の Sun 背景画面 (外周部が非常に暗いものなど) が中央の位置に正確に表示されない場合があります。別の背景を使用するか、画面の左上隅に明るい色のアイコンを配置してください。



ターゲット コマンドによるスクリーンショット (ターゲット スクリーンショット)

[Screenshot from Target server] (ターゲット サーバのスクリーンショット) コマンドを使用すると、ターゲット サーバのスクリーンショットを取得できます。必要に応じて、このスクリーンショットを、選択した場所にビットマップ、JPEG、または PNG ファイルとして保存します。

► ターゲット サーバのスクリーンショットを取得するには、以下の手順に従います。

1. [Video] (ビデオ) の [Screenshot from Target server] (ターゲット サーバのスクリーンショット) を選択するか、ツールバーの [Target Screenshot] (ターゲット スクリーンショット) ボタン をクリックします。
2. [Save] (保存) ダイアログ ボックスで、ファイルを保存する場所を選択し、ファイルに名前を付け、[Files of type] (ファイルの種類) ドロップダウン リストからファイル形式を選択します。
3. [Save] (保存) をクリックしてスクリーンショットを保存します。

最大垂直走査周波数の変更

ターゲットで使用しているビデオ カードでカスタム ソフトウェアが使用されている場合、MPC または VKC を介してターゲットにアクセスするには、垂直走査周波数がターゲットで有効になるように、モニタの最大垂直走査周波数を変更する必要があります。

▶ モニタの垂直走査周波数を調整するには、以下の手順に従います。

1. Windows® では、[画面のプロパティ] ダイアログ ボックスを開き、[設定]、[詳細設定] の順に選択してプラグ アンド プレイのダイアログ ボックスを開きます。
2. [モニタ] タブをクリックします。
3. [画面のリフレッシュ レート] を設定します。
4. [OK] をクリックし、もう一度 [OK] をクリックして設定を適用します。

マウス オプション

デュアル マウス モードでオプションが適切に設定されている場合、2 つのマウス カーソルは同調します。

デュアル マウス モードで、ターゲット サーバを制御しているとき、リモート コンソールには、2 つのマウス カーソルが表示されます。1 つは KSX II クライアント ワークステーションのマウス カーソルで、もう 1 つはターゲット サーバのマウス カーソルです。

この場合、シングル マウス モードとデュアル マウス モードのどちらかを使用できます。

デバイスでは、2 つのマウス カーソルが存在するときに以下のマウス モードが提供されます。

- Absolute (ずれない) (マウス同期)
- Intelligent (インテリジェント) (マウス モード)
- Standard (標準) (マウス モード)

マウス ポインタが KVM Client ターゲット サーバ ウィンドウ内にある場合、マウスの動作やクリックは、接続されているターゲット サーバに直接送信されます。

クライアントのマウス ポインタは、マウスの加速設定により、動作がわずかにターゲット マウス ポインタより先行します。

高速 LAN 接続では、シングル マウス モードでターゲット サーバのポインタのみを表示できます。

この 2 つのモード (シングル マウスとデュアル マウス) は自由に切り替えることができます。

マウス ポインタの同期

マウスが使用されているターゲット サーバをリモートで表示する場合、2 つのマウス カーソルが表示されます。1 つはリモート クライアント ワークステーションのマウス カーソルで、もう 1 つはターゲット サーバのマウス カーソルです。マウス ポインタが Virtual KVM Client ターゲット サーバ ウィンドウ内にある場合、マウスの動作やクリックは、接続されているターゲット サーバに直接送信されます。クライアントのマウス ポインタは、マウスの加速設定により、動作がわずかにターゲット マウス ポインタより先行します。

高速 LAN 接続の場合、Virtual KVM Client のマウス ポインタを無効にしてターゲット サーバのマウス ポインタのみを表示できます。この 2 つのモード（シングル マウスとデュアル マウス）は自由に切り替えることができます。

マウス同期のヒント

マウスの同期を設定するには、以下の手順に従います。

1. 選択したビデオ解像度と垂直走査周波数がデバイスでサポートされていることを確認します。[Virtual KVM Client Connection Info]（Virtual KVM Client 接続情報）ダイアログ ボックスには、デバイスの表示で使用している実際の値が表示されます。
2. KX II および LX デバイスについては、ケーブルの長さが選択したビデオ解像度に指定されている限度内であることを確認します。
3. インストール プロセス中にマウスとビデオが正しく構成されていることを確認します。
4. [Virtual KVM Client auto-sense]（Virtual KVM Client の自動検出）ボタンをクリックして自動検出を強制します。
5. 以上の手順で Linux、UNIX、Solaris KVM ターゲット サーバのマウス同期が改善しない場合は、以下の手順に従います。
    a. ターミナル ウィンドウを開きます。
    b. 次のコマンドを入力します。`xset mouse 1 1`
    c. ターミナル ウィンドウを閉じます。
6. [Virtual KVM Client mouse synchronization]（Virtual KVM Client マウス同期）ボタン をクリックします。

インテリジェント マウス モードでの追加の注意事項

- 同期ルーチンが利用する領域を空けるため、画面の左上隅にアイコンやアプリケーションがないことを確認します。
- アニメーション カーソルを使用しないでください。
- KVM ターゲット サーバでアクティブなデスクトップを無効にします。

マウスの同期

デュアル マウス モードで [Synchronize Mouse] (マウスの同期) コマンドを使用すると、ターゲット サーバのマウス ポインタと Virtual KVM Client のマウス ポインタとの同期化が再実行されます。

▶ マウスを同期するには、次のいずれかの手順に従います。

- [Mouse] (マウス) の [Synchronize Mouse] (マウスの同期) を選択するか、ツールバーの [Synchronize Mouse] (マウスの同期) ボタン をクリックします。

注: このオプションは、標準マウス モードとインテリジェント マウス モードでのみ使用可能です。

標準マウス モード

標準マウス モードは、相対マウス位置を使用した標準のマウス同期アルゴリズムです。標準マウス モードを使用する場合、クライアントとサーバのカーソルが同期するように、マウスの加速を無効にし、マウスに関連するその他のパラメータを適切に設定する必要があります。

▶ 標準マウス モードに切り替えるには、以下の手順に従います。

- [Mouse] (マウス) の [Standard] (標準) を選択します。

インテリジェント マウス モード

デバイスでは、インテリジェント マウス モードにおいて、ターゲットのマウス設定を検出し、それに応じてマウス カーソルを同期できるので、ターゲットでマウスの加速を設定できます。インテリジェント マウス モードは、VM ターゲット以外のデフォルトです。

同期中は、マウス カーソルが画面の左上隅で "ダンス" をし、加速が計算されます。このモードが正常に動作するには、特定の条件が満たされる必要があります。

▶ **インテリジェント マウス モードに切り替えるには、以下の手順に従います。**

- [Mouse] (マウス) の [Intelligent] (インテリジェント) を選択します。

インテリジェント マウス同期の条件

[Mouse] (マウス) メニューにある [Intelligent Mouse Synchronization] (インテリジェント マウス同期) コマンドを選択すると、マウスが動いていないときにマウス カーソルが自動的に同期されます。この機能を適切に動作させるには、次の条件が満たされている必要があります。

- ターゲットにおいて、アクティブ デスクトップが無効であること。
- ターゲット ページの左上隅にウィンドウが表示されていないこと。
- ターゲット ページの左上隅にアニメーション背景が表示されていないこと。
- ターゲットのマウス カーソルが通常のものであり、アニメーション カーソルでないこと。
- ターゲット マウスの速度が、非常に遅い値や非常に速い値に設定されていないこと。
- [ポインタの精度を高める] や [ポインタを自動的に既定のボタン上に移動する] などの高度なマウス プロパティが無効であること。
- [ビデオ設定] ウィンドウで [最適ビデオ モード] を選択していること。
- ターゲットのビデオの外周部が明確に表示されていること (つまり、ターゲットのビデオ画像の端にスクロールしたときに、ターゲット デスクトップとリモート KVM コンソール ウィンドウの間に黒いボーダーが表示されている必要があります)。
- インテリジェント マウス同期機能を使用中に、デスクトップの左上隅にファイル アイコンやフォルダ アイコンがあると、この機能が正しく動作しない可能性があります。この機能での問題を避けるために、デスクトップの左上隅にファイル アイコンやフォルダ アイコンを置かないことを推奨します。

ターゲット ビデオが自動検出された後で、ツール バーの [Synchronize Mouse] (マウス同期) ボタンをクリックして、手動でマウス同期を開始する必要があります。ターゲットの解像度が変更された場合や、マウス カーソルが互いに同期しなくなった場合にも、この操作を行います。

インテリジェント マウス同期が失敗した場合、標準マウス同期と同じ動作になります。

マウス設定は、ターゲットのオペレーション システムよって異なります。詳細については、使用する OS のマニュアルを参照してください。また、インテリジェント マウス同期は UNIX ターゲットでは機能しません。

ずれないマウス モード

このモードでは、ターゲット マウスの加速または速度が異なる値に設定されている場合でも、クライアントとターゲットのカーソルを同期するために絶対座標が使用されます。

このモードは USB ポートを備えたサーバでサポートされ、仮想メディア CIM のデフォルトのモードです。

では、仮想メディア CIM を使用する必要があります。

- D2CIM-VUSB
- D2CIM-DVUSB
- D2CIM-DVUSB-DVI
- D2CIM-DVUSB-HDMI
- D2CIM-DVUSB-DP

▶ ずれないマウス モードに切り替えるには、以下の手順に従います。

- [Mouse] (マウス) の [Absolute] (ずれない) を選択します。

注: ずれないマウス設定を適用するには USB ターゲット システムが必要です。KX II-101 の場合、これが推奨のマウス設定です。

注: KX II デバイスでは、ずれないマウスの同期は、仮想メディア対応の USB CIM (D2CIM-VUSB および D2CIM-DVUSB) でのみ使用可能です。

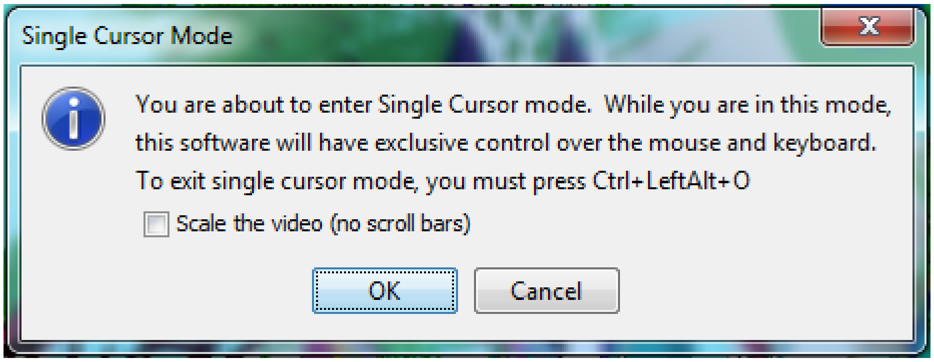
シングル マウス モード

シングル マウス モードでは、ターゲット サーバのマウス カーソルだけを使用します。ローカル マウス ポインタは画面に表示されません。

注:クライアントが仮想マシン上で実行している場合、シングル マウス モードは Windows および Linux のターゲットでは機能しません。

► シングル マウス モードにするには、次のいずれかの手順に従います。

- [Mouse] (マウス) の [Single Mouse Cursor] (シングル マウス カーソル) を選択します。
- ツール バーの [Single/Double Mouse Cursor] (シングル/ダブル マウス カーソル) ボタン をクリックします。



► シングル マウス モードを終了するには、以下の手順に従います。

1. シングル マウス モードを終了するには、キーボードの Ctrl+Alt+O を押します。

VKC 仮想メディア

仮想メディアの設定方法および使用方法についての詳細は、「*仮想メディア* 『*100*p. 』」を参照してください。

スマート カード

サポートされているスマート カード、スマート カード リーダー、およびシステム要件の一覧については、「***サポートされているスマート カード リーダーとサポートされていないスマート カード リーダー***『***310***p. 』」を参照してください。

サーバにリモートでアクセスすると、接続されたスマート カード リーダーを選択し、それをサーバにマウントできます。

スマート カード認証はターゲット サーバで使用されますが、デバイスへのログインには使用されません。したがって、スマート カードの PIN と資格情報を変更するのにデバイス アカウントを更新する必要はありません。 カード リーダーおよびスマート カードをターゲット サーバにマウントすると、サーバはそれらのリーダーやカードが直接接続されているかのように動作します。

スマート カードまたはスマート カード リーダーを取り外すと、ターゲット サーバの OS で設定されているカードの取り外しポリシーに従って、ユーザ セッションがロックされるか、またはユーザがログアウトされます。

KVM セッションが切断されるか、または新しいターゲットに切り替えたために KVM セッションが終了した場合、スマート カード リーダーはターゲット サーバから自動的にマウント解除されます。

デバイスで PC 共有モードを有効にすると、複数のユーザがターゲット サーバへのアクセスを共有できます。ただし、スマート カード リーダーがターゲットに接続されている場合は、PC 共有モードの設定にかかわらず、デバイスによってプライバシーが強化されます。さらに、ターゲット サーバで共有セッションに加わっている場合は、ターゲット サーバへの排他的アクセスが可能になるまでスマート カード リーダーのマウントが無効になります。

ターゲット サーバへの KVM セッションが確立されると、Virtual KVM Client (VKC)、Active KVM Client (AKC)、および Multi-Platform Client (MPC) でスマート カードのメニューとボタンが使用可能になります。メニューを開くか [Smart Card] (スマート カード) ボタンを選択すると、リモート クライアントに接続されているスマート カード リーダーが表示されます。このダイアログ ボックスでは、追加のスマート カード リーダーを接続したり、ターゲット サーバに接続されているスマート カード リーダーのリストを更新したり、スマート カード リーダーの接続を解除したりできます。スマート カードの取り外しと再挿入も行うことができます。この機能を使用して、適切なログイン ダイアログ ボックスを表示するために、カードの取り外しまたは再挿入が必要であるターゲット サーバの OS に通知を送信できます。通知は、他のアクティブな KVM セッションに影響を与えることなく 1 台のターゲット サーバに送信できます。

▶ スマート カード リーダーをマウントするには､以下の手順に従います｡

1. [Smart Card] (スマート カード) メニューをクリックし、[Smart Card Reader] (スマート カード リーダー) を選択します。または、ツールバーの [Smart Card] (スマート カード) ボタン をクリックします。
2. [Select Smart Card Reader] (スマート カード リーダーの選択) ダイアログ ボックスでスマート カード リーダーを選択します。
3. [Mount] (マウント) をクリックします。
4. 進行状況を示すダイアログ ボックスが開きます｡次回ターゲット サーバに接続したときにスマート カード リーダーを自動的にマウントするには、[Mount selected card reader automatically on connection to targets] (選択したカード リーダーをターゲットへの接続時に自動的にマウントする) チェックボックスをオンにします。[OK] をクリックして、マウント処理を開始します。

▶ **[Select Smart Card Reader] (スマート カード リーダーの選択) ダイアログ ボックスのスマート カード リーダーを更新には、以下の手順に従います。**

- 新しいスマート カード リーダーがクライアント PC に接続された場合は、[Refresh List] (リストの更新) をクリックします。

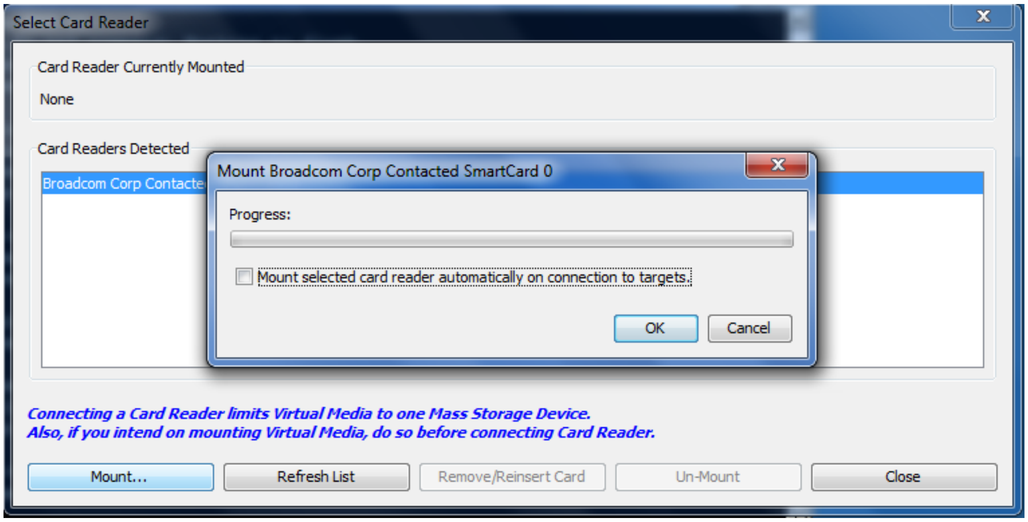
▶ **スマート カードの取り外しおよび再挿入の通知をターゲット サーバに送信するには、以下の手順に従います。**

- 現在マウントされているスマート カード リーダーを選択し、[Remove/Reinsert] (取り外し/再挿入) ボタンをクリックします。

▶ **スマート カード リーダーのマウントを解除するには、以下の手順に従います。**

- マウントを解除するスマート カード リーダーを選択し、[Unmount] (マウント解除) ボタンをクリックします。

ローカル コンソールからのスマート カード リーダーのマウントもサポートされます。詳細については、「**ローカル コンソールのスマート カード アクセス** 『267p. 』」を参照してください。



ツール オプション

[Tools] (ツール) メニューで、Virtual KVM Client 用の特定のオプションを指定できます。このオプションには、ログ作成、キーボードの種類の設定、全画面モードやシングル カーソル モードを終了するホットキーの定義などがあります。

注:KX II-101 および KX II-101-V2 は、シングル カーソル モードをサポートしていません。

ツール オプションを設定するには、以下の手順に従います。

1. [Tools] (ツール) の [Options] (オプション) を選択します。[オプション] ウィンドウが表示されます。
2. テクニカル サポートから指示されたときだけ、[Enable Logging] (ログ記録を有効にする) チェックボックスをオンにします。このオプションをオンにすると、ホーム ディレクトリにログ ファイルが作成されます。
3. 必要に応じて、ドロップダウン リストからキーボードの種類を選択します。含まれるオプションは次のとおりです。
   - 英語 (アメリカ)/(インターナショナル)
   - フランス語 (フランス)
   - ドイツ語 (ドイツ)
   - 日本語
   - 英語 (イギリス)
   - 韓国語 (韓国)
   - フランス語 (ベルギー)
   - ノルウェー語(ノルウェー)
   - ポルトガル語 (ポルトガル)
   - デンマーク語 (デンマーク)
   - スウェーデン語 (スウェーデン)
   - ドイツ語 (スイス)
   - ハンガリー語 (ハンガリー)
   - スペイン語 (スペイン)
   - イタリア語 (イタリア)
   - スロベニア語
   - 変換 – フランス語 – US 英語
   - 変換 – フランス語 – US インターナショナル

   注:AKC では、キーボードの種類のデフォルトがローカル クライアントになるので、このオプションは適用されません。

   注:KX II-101 は AKC をサポートしていません。

4. [Exit Full Screen Mode] (全画面モードの終了) - ホットキー。全画面モードに切り替えると、ターゲット サーバの表示が全画面表示になり、ターゲット サーバと同じ解像度が取得されます。これは、このモードを終了するためのホットキーです。
5. [Exit Single Cursor Mode] (シングル カーソル モードの終了) - ホットキー。シングル カーソル モードに入ると、ターゲット サーバのマウス カーソルのみが表示されます。これは、シングル カーソル モードを終了してクライアント マウス カーソルを復活させるホットキーです。[OK] をクリックします。
6. **クライアント起動設定**
7. [Client Launch Settings] (クライアント起動設定) タブを選択します。
    a. ターゲット ウィンドウ設定をカスタマイズするには
    - ターゲットの現在の解像度に合ったサイズのウィンドウを開くには、[Standard - sized to target Resolution] (標準 - ターゲットの解像度に合わせる) を選択します。ターゲットの解像度がクライアントの解像度よりも高い場合、画面全体にターゲット ウィンドウが表示され、表示しきれない部分がある場合は、スクロール バーが追加表示されます。
    - ウィンドウを全画面モードで開くには、[Full Screen] (全画面) を選択します。

    a. ターゲット ビューアが起動するモニタをカスタマイズするには
    - クライアント上で使用されているアプリケーション (例: Web ブラウザ、アプレット) を表示しているモニタと同じモニタを使用してターゲット ビューアを起動するには、[Monitor Client Was Launched from] (クライアントが起動されているモニタ) を選択します。
8. アプリケーションによって現在検出されているターゲット モニタの一覧から選択するには、[Select From Detected Monitors] (検出されたモニタの中から選択) を選択します。以前選択したモニタが検出されなくなった場合、"Currently Selected Monitor Not Detected" (現在選択されているモニタが検出されませんでした) というメッセージが表示されます。
9. [OK] をクリックします。

キーボードの制限

スロベニア語キーボード

JRE の制限により、< キーは、スロベニア語キーボードでは機能しません。

Linux での言語設定

Linux 上の Sun JRE では、システムの環境設定を使用して設定される外国語のキーボードで正しいキー イベントを生成する際に問題があるので、外国語キーボードは、次の表で説明する方法を使用して設定することをお勧めします。

言語	設定方法
アメリカ英語/国際	デフォルト設定
フランス語	Keyboard Indicator
ドイツ語	[System Settings] (システム設定) (Control Center)
日本語	[System Settings] (システム設定) (Control Center)
イギリス英語	[System Settings] (システム設定) (Control Center)
韓国語	[System Settings] (システム設定) (Control Center)
ベルギー語	Keyboard Indicator
ノルウェー語	Keyboard Indicator
デンマーク語	Keyboard Indicator
スウェーデン語	Keyboard Indicator
ハンガリー語	[System Settings] (システム設定) (Control Center)
スペイン語	[System Settings] (システム設定) (Control Center)
イタリア語	[System Settings] (システム設定) (Control Center)
スロベニア語	[System Settings] (システム設定) (Control Center)
ポルトガル語	[System Settings] (システム設定) (Control Center)

注: デスクトップ環境として Gnome を使用している Linux システムでは、Keyboard Indicator を使用してください。

表示オプション

[View Toolbar] (ツール バーの表示)

Virtual KVM Client では、ツール バーの表示/非表示を切り替えることができます。

▶ ツール バーの表示/非表示 (オン/オフ) を切り替えるには、以下の手順に従います。

- [View] (表示) の [View Toolbar] (ツール バーの表示) を選択します。

[Scaling] (拡大、縮小)

ターゲットのウィンドウを拡大、縮小することで、ターゲット サーバ ウィンドウ全体の内容を表示することができます。

Virtual KVM Client のウィンドウ サイズに合わせて、縦横比を維持したまま、ターゲット ビデオのサイズを拡大または縮小することができるため、スクロール バーを使用することなくターゲット サーバのデスクトップ全体を表示することができます。

▶ 拡大、縮小 (オン/オフ) を切り替えるには、以下の手順に従います。

- [View] (表示) の [Scaling] (拡大、縮小) を選択します。

[Target Screen Resolution] (ターゲット画面解像度)

全画面モードに切り替えると、ターゲットの全画面が表示され、ターゲット サーバと同じ解像度になります。このモードを終了するためのホットキーは、[Options] (オプション) ダイアログ ボックスで指定します (デフォルトは Ctrl+Alt+M です)。全画面モードになっているときに、マウス ポインタを画面上端に移動すると、全画面モード メニュー バーが表示されます。

▶ 全画面モードに切り替えるには、以下の手順に従います。

- [View] (表示) の [Full Screen] (全画面) を選択します。

▶ 全画面モードを終了するには、以下の手順に従います。

- [Tools] (ツール) の [Options] (オプション) ダイアログで設定されているホットキーを押します。デフォルトのホット キーは Ctrl+Alt+M です。AKC の場合、マウス ポインタを画面上端に移動して、非表示になっているメニュー バーを表示し、[Connection/Exit] (接続/終了) を選択します。

注:KX II-101 は AKC をサポートしていません。

あるいは、常に全画面モードでターゲットにアクセスする場合は、全画面モードをデフォルトにすることができます。

▶ **全画面モードをデフォルトのモードとして設定するには、以下の手順に従います。**

1. [Tools] (ツール) の [Options] (オプション) をクリックして [Options] (オプション) ダイアログ ボックスを開きます。
2. [Enable Launch in Full Screen Mode] (全画面モードで開く) を選択して [OK] をクリックします。

バージョン情報 - Virtual KVM Client

このメニュー コマンドを選択すると、Virtual KVM Client のバージョン情報が表示されます。このバージョン情報は、ラリタン テクニカル サポートを利用するときに必要になります。

▶ **バージョン情報を調べるには、以下の手順に従います。**

1. [Help] (ヘルプ) の [About Raritan Virtual KVM Client] (バージョン情報) を選択します。
2. 後でサポート時にアクセスできるように、[Copy to Clipboard] (クリップボードにコピー) ボタンを使用して、ダイアログ ボックスに含まれている情報をクリップボード ファイルにコピーします (必要な場合)。

Active KVM Client (AKC)

このクライアントは Raritan の各種製品で使用されていることに注意してください。このように、ヘルプのこのセクションには、他の製品への参照が表示される場合があります。

概要

- AKC は Microsoft Windows .NET 技術に基づいています。したがって、Raritan の VKC および MPC の実行に必要な Java Runtime Environment (JRE) を使用することなくクライアントを Windows 環境で実行できます。AKC は CC-SG とも連動します。

アプリケーションの利用可能な機能の使用方法については、「*Virtual KVM Client* 『*61*p. の"*Virtual KVM Client (VKC)*"参照 』」セクションを参照してください。AKC の動作と VKC の動作の違いが記載されています。

AKC の使用に関する設定情報については、「*ダイレクト ポート アクセスの有効化* 『*156*p. の"*URL を経由したダイレクト ポート アクセスの有効化*"参照 』」および「*AKC ダウンロード サーバ証明書の検証の有効化* 『*159*p. 』」も参照してください。

注: AKC でダイレクト ポート アクセスを使用する場合は、アクセスするターゲットごとに新しいブラウザ ウィンドウまたはブラウザ タブを開く必要があります。現在ターゲットへのアクセスに使用しているのと同じブラウザ ウィンドウまたはブラウザ タブに DPA URL を入力して別のターゲットにアクセスしようとすると、接続できずにエラーが表示される場合があります。

AKC でサポートされている .NET Framework、オペレーティング システムとブラウザ

.NET Framework

AKC には、Windows .NET® バージョン 3.5 または 4.0 が必要です。AKC は、インストールされている 3.5 および 4.0 の両方と連動します。

オペレーティング システム

AKC は、以下のプラットフォームに対応しています。

- Windows XP® オペレーティング システム
- Windows Vista® (64 ビット版も可)
- Windows 7® (64 ビット版も可)
- Windows 8® (64 ビット版も可)

注: WINDOWS PC FIPS を有効にし、かつ、AKC とスマート カードを使用してターゲットにアクセスする場合、Windows 7 を使用する必要があります。

AKC を実行するには .NET が必要になるため、.NET がインストールされていない場合、またはサポートされていないバージョンの .NET がインストールされている場合は、.NET バージョンの確認を指示するメッセージが表示されます。

注: Windows XP® オペレーティング システムのユーザは、AKC を起動する前に、基盤となる .NET 3.5 または 4.0 がインストールされているか確認することをお勧めします。.NET バージョンが機能していることを確認できない場合は、.NET バージョンの確認を求めるデフォルトのメッセージが表示される代わりにファイルをダ ウンロードするよう求められる場合があります。

ブラウザ

- Internet Explorer 6 以降

IE 6 以降ではないブラウザから AKC を開こうとすると、ブラウザの確認と Internet Explorer への切り替えを指示するエラー メッセージが表示されます。

AKC を使用するための必要条件

AKC を使用するには、以下の手順に従います。

- アクセスするデバイスの IP アドレスからの Cookie が現在ブロックされていないことを確認します。
- Windows Vista、Windows 7、および Windows 2008 Server のユーザは、アクセスするデバイスの IP アドレスがブラウザの［信頼済みサイト］ゾーンに含まれ、デバイスへのアクセス時に保護モードが有効になっていないことを確認する必要があります。

AKC ダウンロード サーバ証明書の検証を有効にする

デバイス（または CC-SG）の管理者が［Enable AKC Download Server Certificate Validation (AKC ダウンロード サーバ証明書の検証を有効にする)］オプションを有効にした場合は、以下の手順に従います。

- 管理者は、有効な証明書をデバイスにアップロードするか、自己署名証明書をデバイスで生成する必要があります。証明書で有効なホストが指定されている必要があります。
- 各ユーザは、CA 証明書（または自己署名証明書のコピー）をブラウザの信頼されたルート証明機関ストアに追加する必要があります。

CC-SG Admin Client から AKC を起動する場合は、JRE™ 1.6.0_10 以上が必要です。

Multi-Platform Client (MPC)

Raritan Multi-Platform Client (MPC) は、Raritan 製品ラインに対応するグラフィカル ユーザ インタフェースです。Raritan KVM over IP デバイスに接続されているターゲット サーバへのリモート アクセスを提供します。MPC の使用方法については、Raritan の Web サイトでユーザ ガイドと同じページから入手できる『KVM and Serial Access Client Guide』を参照してください。MPC の起動手順が記載されています。

このクライアントは Raritan の各種製品で使用されていることに注意してください。このように、ヘルプのこのセクションには、他の製品への参照が表示される場合があります。

Web ブラウザからの MPC の起動

重要: ブラウザの種類を問わず、MPC を開くためには、Dominion デバイスの IP アドレスからのポップアップを許可する必要があります。

重要: Intel® プロセッサを搭載した Mac OS X 10.5/10.6 コンピュータは JRE 1.6 を実行できるので、クライアントとして使用できます。Mac OS X 10.5.8 は、スタンドアロン クライアントとして MPC をサポートしていません。

1. サポートされるブラウザを実行しているクライアントから MPC を開くには、アドレス フィールドに「http://IP-ADDRESS/mpc」と入力します (IP-ADDRESS はラリタン デバイスの IP アドレスに置き換えてください)。MPC が新しいウィンドウに開かれます。

   注: Alt+Tab コマンドで、ローカル システム上のウィンドウ間のみでの切り替えができます。

   MPC が開かれると、自動的に検出されたラリタン デバイスおよびサブネット上で見つかったラリタン デバイスがナビゲータにツリー形式で表示されます。

2. 使用しているデバイスの名前がナビゲータに表示されていない場合は、以下の手順に従って手動で追加します。
   a. [Connection] (接続)、[New Profile] (新しいプロファイル) の順に選択します。[Add Connection] (接続の追加) ウィンドウが開きます。
   b. [Add Connection] (接続の追加) ウィンドウで、デバイスの説明を入力し、接続タイプを指定し、デバイスの IP アドレスを追加して、[OK] をクリックします。この指定内容は後で編集できます。
3. 画面左のナビゲータ パネルで、接続するラリタン デバイスに対応するアイコンをダブルクリックします。

注: お使いのブラウザおよびブラウザのセキュリティ設定によっては、さまざまなセキュリティや証明書に関する確認メッセージまたは警告メッセージが表示されることがあります。MPC を開くには、オプションを承諾する必要があります。

注: Firefox 3.0.3 を使用している場合は、アプリケーションの起動で問題が発生することがあります。この場合は、ブラウザのキャッシュをクリアして、アプリケーションを再起動してください。

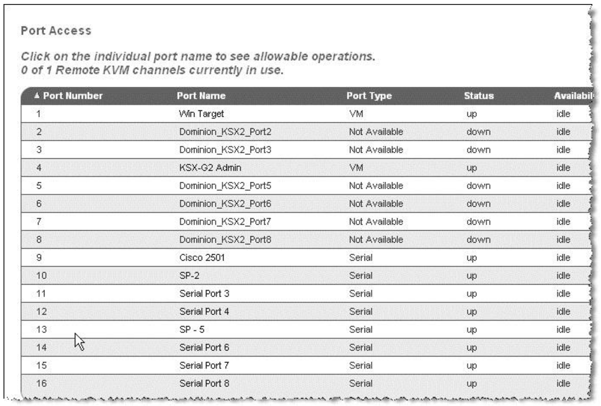
Raritan Serial Console (RSC)

スタンドアロン Raritan Serial Console (RSC) は、デバイスを経由せずにシリアル ターゲットへの直接接続を行うために使用されます。ユーザがデバイスのアドレスとポート番号 (ターゲット) を指定すると、接続されます。

リモート コンソールから RSC を開く

▶ **リモート コンソールから Raritan Serial Console (RSC) を開くには、以下の手順に従います。**

1. [Port Access] (ポート アクセス) タブを選択します。



Port Access

Click on the individual port name to see allowable operations.
0 of 1 Remote KVM channels currently in use.

▲ Port Number	Port Name	Port Type	Status	Availabil
1	Win Target	VM	up	idle
2	Dominion_KSX2_Port2	Not Available	down	idle
3	Dominion_KSX2_Port3	Not Available	down	idle
4	KSX-G2 Admin	VM	up	idle
5	Dominion_KSX2_Port5	Not Available	down	idle
6	Dominion_KSX2_Port6	Not Available	down	idle
7	Dominion_KSX2_Port7	Not Available	down	idle
8	Dominion_KSX2_Port8	Not Available	down	idle
9	Cisco 2501	Serial	up	idle
10	SP-2	Serial	up	idle
11	Serial Port 3	Serial	up	idle
12	Serial Port 4	Serial	up	idle
13	SP - 5	Serial	up	idle
14	Serial Port 6	Serial	up	idle
15	Serial Port 7	Serial	up	idle
16	Serial Port 8	Serial	up	idle

2. RSC でアクセスするシリアル ポートの名前をクリックします。

   注: RSC への接続に https を使用した場合にのみ、セキュリティ ポップアップ画面が開きます。

3. Dominion DSX を使用する場合:
   - [Yes] (はい) をクリックします。[Warning – Security] (警告 – セキュリティ) 画面が表示されます。
   - [Yes] (はい) をクリックし、[Port] (ポート) ページから Raritan Serial Console にアクセスします。

   注: [Always] (常にはい) をクリックすると、今後アクセスするときにセキュリティ ページは表示されなくなります。

- [Raritan Serial Console] ウィンドウが表示されます。

Dominion KSX または KX を使用する場合:

- [Connect] (接続) をクリックして RSC のターゲット ポートへの接続を開始すると、[Raritan Serial Console] ウィンドウが開きます。
- [Raritan Serial Console] ウィンドウが表示されます。

注: Raritan の Web サイト (www.raritan.com) のサポート ページから、スタンドアロンの Raritan Serial Console をダウンロードすることもできます。

▶ Windows® デスクトップから RSC を開くには、以下の手順に従います。

1. ショートカットをダブルクリックするか、[スタート] メニューからスタンドアロンの RSC を開きます。Raritan Serial Console の [Login] (ログイン) 接続プロパティ ウィンドウが表示されます。
2. デバイスの IP アドレス、アカウント情報、および目的のターゲット (ポート) を入力します。
3. [Start] (開始) をクリックします。ポートに接続された状態で RSC が開きます。

注: ローカリゼーション サポートが原因で RSC ウィンドウに読めない文字やぼやけたページがある場合、フォントを Courier New に変更してみてください。[Emulator] (エミュレータ)、[Settings] (設定)、[Display] (表示) をクリックし、[Terminal Font Properties] (ターミナル フォント プロパティ) または [GUI Font Properties] (GUI フォント プロパティ) で [Courier New] を選択します。

注: RSC がシリアル ターゲットに接続しているときは、Ctrl + _ キーまたは Ctrl + ˆ + _ キーを押しても情報は送信されません。ただし、Ctrl + Shift + _ キーまたは Ctrl + Shift + ˆ キーを押すと、情報が送信されます。

▶ Sun™ Solaris™ で RSC を開くには、以下の手順に従います。

1. ターミナル ウィンドウを開き、RSC をインストールしたディレクトリに移動します。
2. 「`./start.sh`」と入力して *Enter* キーを押し、*RSC* を開きます。
3. 目的のデバイスをダブルクリックして、接続を確立します。
4. ユーザ名とパスワードを入力します。
5. [OK] をクリックして、ログオンします。

Ch 4　ラック PDU (電源タップ) のコンセントの制御

この章の内容

概要 97
コンセントの電源オン/オフの切り替えまたは電源再投入を行う......... 98

概要

KSX II では、Raritan PX および RPC シリーズのラック PDU (電源タップ) コンセントを制御できます。. PX または RPC シリーズをセットアップして KSX II に接続すると、そのラック PDU および各コンセントを KSX II のユーザ インタフェース (UI) 画面の [Powerstrip] (電源タップ) ページで制御できるようになります。このページを開くには、UI の上端にある [Power] (電源) メニューをクリックします。

[Powerstrip] (電源タップ) ページが開きます。このページには、KSX II に接続されており、かつ、ユーザが適切なポートアクセス権限を付与されている、ラック PDU が表示されます。

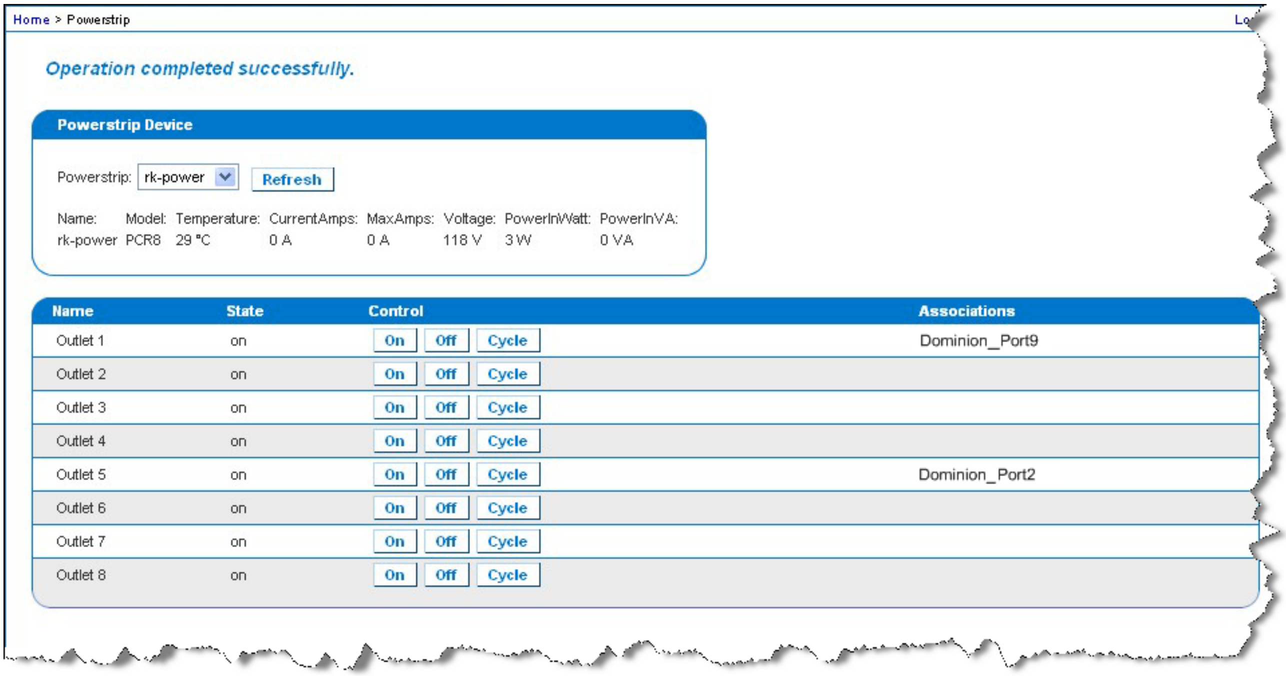
注:PX のセットアップ手順については、『Raritan PX User Guide (Raritan PX ユーザ ガイド)』を参照してください。

[Powerstrip] (電源タップ) ページでは、各コンセントの電源のオン/オフを切り替えること、および、各コンセントの電源を再投入することができます。また、電源タップおよび各コンセントに関する次の情報を表示できます。

- 電源タップに関する情報:
  - [Name] (名前)
  - [Model] (モデル)
  - 温度
  - 電流 (A)
  - 最大電流 (A)
  - 電圧 (V)
  - 電力 (W)
  - 電力 (VA)
- コンセントに関する情報:
  - [Name] (名前): 設定時にコンセントに割り当てた名前。
  - [State] (状態): コンセントの状態 ("on" (オン) または "off" (オフ))。

- [Control] (制御): コンセントの電源を制御するボタン ([On] (オン)、[Off] (オフ)、および [Cycle] (電源再投入))。
- [Association] (関連ポート): コンセントに関連付けられているポート。

[Powerstrip] (電源タップ) ページを開くと、KSX II に接続されている電源タップが [Powerstrip] (電源タップ) ボックスの一覧に表示されます。また、そのボックスに、現在選択されている電源タップに関する情報が表示されます。KSX II に接続されている電源タップが 1 台もない場合は、このページの [Powerstrip Device] (電源タップ) セクションに "No powerstrips found" (電源タップが見つかりません) というメッセージが表示されます。



コンセントの電源オン/オフの切り替えまたは電源再投入を行う

▶ コンセントの電源をオンにするには

1. [Power] (電源) メニューをクリックし、[Powerstrip] (電源タップ) ページを開きます。
2. [Powerstrip] (電源タップ) ボックスの一覧で、コンセントの電源をオンにする PX ラック PDU (電源タップ) を選択します。
3. [Refresh] (最新の情報に更新) ボタンをクリックし、各電源制御ボタンを表示します。

4. 電源をオンにするコンセントの横の [On] (オン) をクリックします。
5. 電源オン完了ダイアログ ボックスが開くので、[OK] をクリックして閉じます。コンセントの電源がオンになり、[State] (状態) 列の表示が "on" (オン) になります。

▶ コンセントの電源をオフにするには

1. 電源をオフにするコンセントの横の [Off] (オフ) をクリックします。
2. 電源オフ確認ダイアログ ボックスが開くので、[OK] をクリックして閉じます。
3. 電源オフ完了ダイアログ ボックスが開くので、[OK] をクリックして閉じます。コンセントの電源がオフになり、[State] (状態) 列の表示が "off" (オフ) になります。

▶ コンセントの電源を再投入するには

1. 電源を再投入するコンセントの横の [Cycle] (電源再投入) をクリックします。電源再投入確認ダイアログ ボックスが開きます。
2. [OK] をクリックします。コンセントの電源が再投入されます。電源再投入には数秒かかることがあります。
3. 電源再投入が完了すると、電源再投入完了ダイアログ ボックスが開きます。[OK] をクリックしてこのダイアログ ボックスを閉じます。

Ch 5 仮想メディア

この章の内容

概要 101
仮想メディアを使用するための条件 104
Windows 環境での VKC および AKC を介した仮想メディア 106
仮想メディアの使用 107
仮想メディア ファイル サーバのセットアップ (ファイル サーバ ISO イメージの場合のみ) 109
仮想メディアへの接続 111
仮想メディアの切断 114

概要

KVM の機能を拡張する仮想メディアを使うことで、クライアント PC やネットワーク ファイル サーバ上のメディアに、リモートの KVM ターゲット サーバからアクセスできるようになります。この機能を使用すると、クライアント PC やネットワーク ファイル サーバでマウントされたメディアが、ターゲット サーバでも仮想的にマウントされます。これにより、そのメディアはターゲット サーバ自体に物理的に接続されているような形で読み書きできるようになります。仮想メディアによるデータ ファイルのサポートに加え、USB 接続を介した仮想メディアによるファイルのサポートもあります。

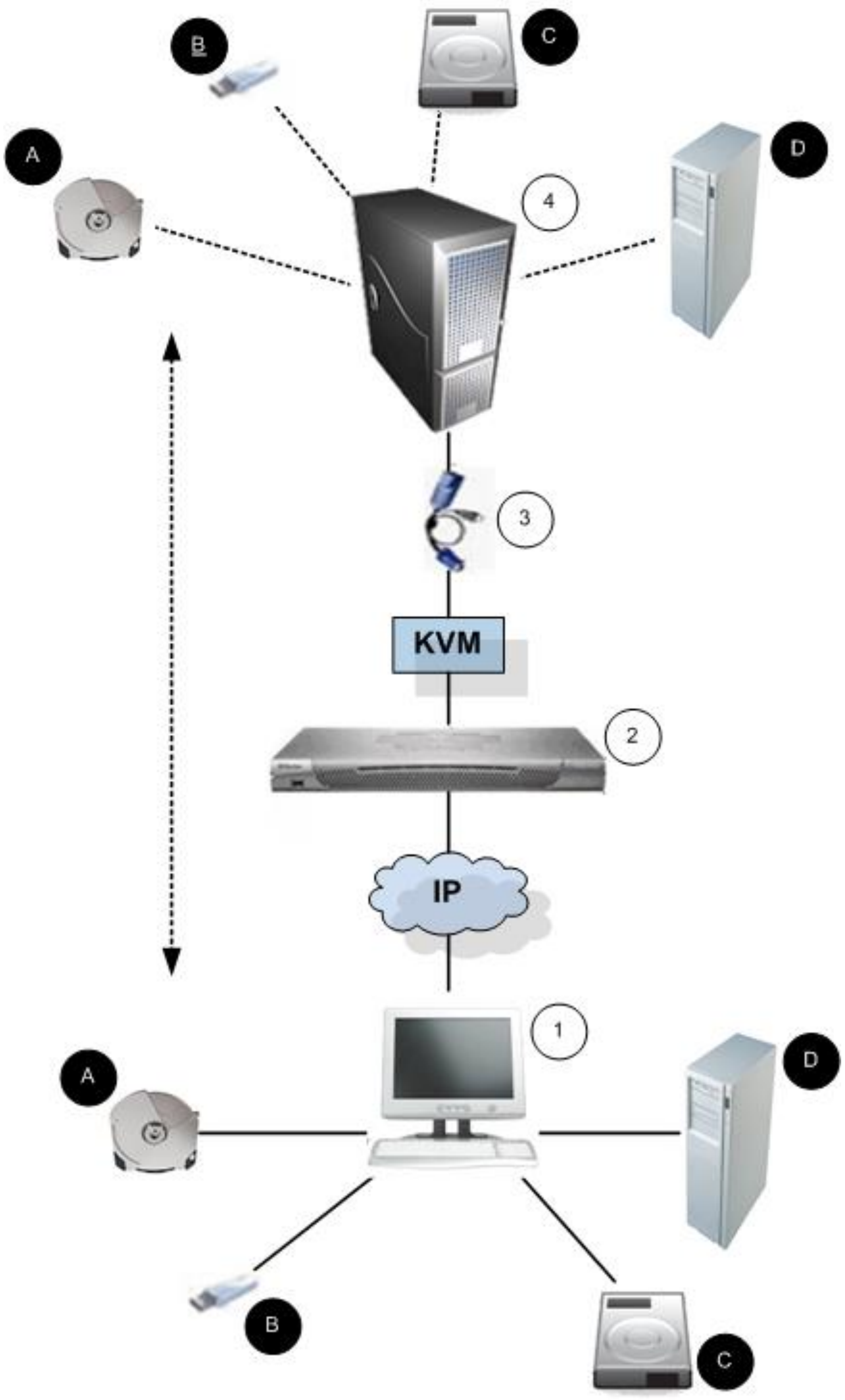
仮想メディアには、内蔵または USB マウントされた CD ドライブや DVD ドライブ、USB マス ストレージ デバイス、PC のハード ディスク ドライブ、ISO イメージ (ディスク イメージ) などを使用できます。

注: ラリタンは ISO9660 を標準でサポートしています。ただし、他の ISO 標準も使用できます。

仮想メディアを使用することで、以下のような作業をリモートから実行できるようになります。

- ファイルの転送
- 診断の実行
- アプリケーションのインストールと修正パッチ (patch) の適用
- オペレーティング システムの完全インストール

この拡張 KVM コントロールを利用することで、データ センタに出向く必要がなくなり、時間と費用の節約になります。このように、仮想メディアは非常に有用な機能です。


B
C
A
D
4
3
KVM
2
IP
1
A
D
B
C

図の説明			
1	デスクトップ PC	A	CD/DVD ドライブ
2	KSX II	B	USB マス ストレージ デバイス
3	CIM	C	PC ハード ディスク ドライブ
4	ターゲット サーバ	D	リモート ファイル サーバ (ISO イメージ)

仮想メディアを使用するための条件

仮想メディア機能では、現在ターゲットに適用されている USB プロファイルがサポートする最大 2 台のドライブ（異なるタイプ）をマウントできます。このドライブは、KVM セッションの間のみアクセスできます。

たとえば、特定の CD-ROM をマウントして、それを使用し、作業が終了したらアンマウントすることができます。それでも、別の CD-ROM を仮想的にマウントできるように、この CD-ROM 仮想メディアの "チャンネル" は開いたままになります。こうした仮想メディアの "チャンネル" は、USB プロファイルでサポートされている限り、KVM セッションが閉じられるまで開いたままになります。

仮想メディアを使用するには、ターゲット サーバからアクセスするメディアをクライアントまたはネットワーク ファイル サーバに接続します。この手順を最初に行う必要はありませんが、このメディアへのアクセスを試行する前に行う必要があります。

仮想メディアを使用するには、次の条件が満たされている必要があります。a

Dominion デバイス

- 仮想メディアへのアクセスを要求するユーザに対して、該当するポートへのアクセスや、これらのポートの仮想メディア アクセス（VM アクセス ポート権限）を許可するようにデバイスを設定する必要があります。ポート権限はグループレベルで設定されます。
- デバイスとターゲット サーバ間に USB 接続が存在する必要があります。
- PC 共有を使用する場合は、[Security Settings]（セキュリティ設定）ページで***セキュリティ設定*** 『*207*p. の"***セキュリティの設定***"参照 』を有効にする必要があります。**(オプション)**
- 接続先の KVM ターゲット サーバの適切な USB プロファイルを選択する必要があります。

クライアント PC

- 仮想メディアの一部のオプションを使用するには、クライアント PC に対する管理者特権が必要です（ドライブ全体のドライブ リダイレクト機能など)。

> *注:Microsoft Vista または Windows 7 を使用している場合は、ユーザー アカウント制御を無効にするか、Internet Explorer を起動するときに [管理者として実行] を選択します。このためには、[スタート] メニューの [Internet Explorer] を右クリックし、[管理者として実行] を選択します。*

ターゲット サーバ

- KVM ターゲット サーバは USB 接続のドライブをサポートする必要があります。
- Windows 2000 が動作する KVM ターゲット サーバには､最新の修正プログラムがすべてインストールされている必要があります。
- USB 2.0 の方が高速なため、推奨されます。

Windows 環境での VKC および AKC を介した仮想メディア

Windows XP® の Administrator 権限および標準ユーザ権限は、Windows Vista® および Windows 7® とは異なります。

Vista または Windows 7 でユーザ アクセス制御 (UAC) を有効にすると、ユーザがアプリケーションの実行に必要とする最低レベルの権限が与えられます。たとえば、Internet Explorer® でユーザに管理者レベルのタスクの実行を明示的に許可するための [管理者として実行] オプションが用意されています。このオプションを使用しない場合、ユーザは管理者としてログインしていても管理者レベルのタスクを実行できません。

どちらの機能も、ユーザが Virtual KVM Client (VKC) および Active KVM Client (AKC) を使用してアクセスできる仮想メディアのタイプに影響します。これらの機能の詳細および使用方法については、Microsoft® のヘルプを参照してください。

ユーザが Windows 環境で VKC および AKC を使用してアクセスできる仮想メディアのタイプを以下に示します。機能をクライアント別に分類し、各 Windows ユーザ役割がアクセスできる仮想メディア機能を示します。

Windows XP

VKC および AKC を Windows XP 環境で実行している場合、CD-ROM 接続、ISO、および ISO イメージを除く仮想メディア タイプにアクセスするには、ユーザに管理者権限が必要です。

Windows Vista および Windows 7

VKC および AKC を Windows Vista または Windows 7 環境で実行し、UAC が有効になっている場合は、ユーザの Windows 役割に応じて以下の仮想メディア タイプにアクセスできます。

クライアント	管理者	標準ユーザ
AKC および VKC	アクセス先: • 固定ドライブと固定ドライブ パーティション • リムーバブル ドライブ • CD/DVD ドライブ • ISO イメージ • リモート ISO イメージ	アクセス先: • リムーバブル ドライブ • CD/DVD ドライブ • ISO イメージ • リモート ISO イメージ

仮想メディアの使用

KSX II 仮想メディア機能を使用する場合、異なる種類のドライブを 2 台までマウントできます。このドライブは、KVM セッションの間のみアクセスできます。

たとえば、特定の CD-ROM をマウントして、それを使用し、作業が終了したら切断することができます。それでも、別の CD-ROM を仮想的にマウントできるように、この CD-ROM 仮想メディアの "チャンネル" は開いたままになります。このような仮想メディアの "チャンネル" は、KVM セッションが閉じられるまで開いたままになっています。

► 仮想メディアを使用するには、以下の手順に従います。

1. ターゲット サーバからアクセスできるようにするメディアを、クライアントまたはネットワーク ファイル サーバに接続します。この手順を最初に行う必要はありませんが、このメディアにアクセスする前に行う必要があります。
2. 適切な前提条件が満たされていることを確認します。「***仮想メディアを使用するための前提条件***『***104***p. の"***仮想メディアを使用するための条件***"参照 』」を参照してください。
3. 仮想メディアを使用するには、次の条件が満たされている必要があります。

KSX II

- 仮想メディアへのアクセスを要求するユーザに対して、該当するポートへのアクセスや、これらのポートの仮想メディア アクセス (VM アクセス ポート権限) を許可するように KSX II を設定する必要があります。ポート権限はグループレベルで設定されます。詳細は、ユーザ ガイドの「ポート権限の設定」を参照してください。
- KSX II デバイスとターゲット サーバ間に USB 接続が存在する必要があります。
- PC 共有を使用する場合は、[Security Settings] (セキュリティ設定) ページで***セキュリティ設定***『***207***p. の"***セキュリティの設定***"参照 』を有効にする必要があります。**(オプション)**
- 接続先の KVM ターゲット サーバの適切な USB プロファイルを選択する必要があります。

クライアント PC

- 仮想メディアの一部のオプションを使用するには、クライアント PC に対する管理者特権が必要です (ドライブ全体のドライブ リダイレクト機能など)。

注: Microsoft® Vista を使用している場合は、[ユーザ アカウント制御] をオフにする必要があります。[コントロール パネル]、[ユーザ アカウント] の順に選択し、[ユーザ アカウント制御] をオフにします。

Vista アカウントの許可を変更したくない場合は、Internet Explorer® を管理者として実行します。このためには、[スタート] メニューの [Internet Explorer] を右クリックし、[管理者として実行] を選択します。

ターゲット サーバ

- KVM ターゲット サーバは USB 接続のドライブをサポートする必要があります。
- Windows 2000® オペレーティング システムが稼動する KVM ターゲット サーバには、最新の修正プログラムがすべてインストールされている必要があります。

1. USB 2.0 ポートの方が高速なため、推奨されます。
2. ファイル サーバ ISO イメージにアクセスする場合は、KSX II リモート コンソールの [File Server Setup] (ファイル サーバのセットアップ) ページを使用して、ファイル サーバとイメージを指定してください。「***ファイル サーバのセットアップ (ファイル サーバ ISO イメージの場合のみ)*** 『***109***p. の"***仮想メディア ファイル サーバのセットアップ (ファイル サーバ ISO イメージの場合のみ)***"参照先 』」を参照してください。

注: Raritan は ISO9660 形式を標準でサポートしています。ただし、その他の CD-ROM 拡張でも動作します。

3. 適切なターゲット サーバとの KVM セッションを開きます。
   a. KSX II リモート コンソールで [Port Access] (ポート アクセス) ページを開きます。
   b. [Port Access] (ポート アクセス) ページでターゲット サーバに接続します。
   - 適切なサーバのポート名をクリックします。
   - [Port Action] (ポート アクション) メニューの [Connect] (接続) コマンドを選択します。[***Virtual KVM Client*** 『***61***p. の"***Virtual KVM Client (VKC)***"参照 』] (仮想 KVM クライアント) ウィンドウにターゲット サーバが表示されます。
4. 仮想メディアに接続します。

対象メディア	この VM オプションを選択
ローカル ドライブ	[Connect Drive] (ドライブの接続)
ローカル CD/DVD ドライブ	***[Connect CD-ROM/ISO Image] (CD-ROM/ISO イメージに接続)*** 『***113***p. の"***CD-ROM/DVD-ROM/ISO イメージ***"参照先 』
ISO イメージ	[Connect CD-ROM/ISO Image]

対象メディア	この **VM** オプションを選択
	(CD-ROM/ISO イメージに接続)
ファイル サーバ ISO イメージ	[Connect CD-ROM/ISO Image] (CD-ROM/ISO イメージに接続)

5. 作業が終わったら、仮想メディアを切断します。「***仮想メディアの切断*** 『*114*p. 』」を参照してください。

仮想メディア ファイル サーバのセットアップ (ファイル サーバ ISO イメージの場合のみ)

この機能は、仮想メディアを使用してファイル サーバ ISO イメージにアクセスする場合にのみ必要です。Raritan は ISO9660 形式を標準でサポートしています。ただし、その他の CD-ROM 拡張でも動作します。

注:ファイル サーバには、SMB/CIFS のサポートが必要です。

リモート コンソールの [File Server Setup] (ファイル サーバのセットアップ) ページで、仮想メディアを使用してアクセスするファイル サーバとイメージのパスを指定します。ここで指定されたファイル サーバ ISO イメージは、[Remote Server ISO Image] (リモート サーバの ISO イメージ) で [Hostname] (ホスト名) および [Image] (イメージ) ドロップダウン リスト ([Map Virtual Media CD/ISO Image] (仮想メディア CD/ISO イメージの割り当て) ダイアログ ボックス) の選択肢として表示されます。「CD-ROM/DVD-ROM/ISO イメージのマウント」を参照してください。

► **仮想メディアとしてアクセスするファイル サーバ ISO イメージを指定するには、以下の手順に従います。**

1. リモート コンソールから仮想メディアを選択します。[File Server Setup] (ファイル サーバのセットアップ) ページが開きます。
2. 仮想メディアとしてアクセスするすべてのメディアについて、[Selected] (選択) チェックボックスをオンにします。
3. アクセスするファイル サーバ ISO イメージに関する情報を入力します。
   - [IP Address/Host Name] (IP アドレス/ホスト名) - ファイル サーバのホスト名または IP アドレスです。
   - [Image Path] (イメージのパス) - ISO イメージの場所を表す完全パス名です。たとえば、/sharename0/path0/image0.iso、¥sharename1¥path1¥image1.iso などです。

   注:ホスト名は 232 文字以内で指定してください。

4. [Save] (保存) をクリックします。これで、指定したすべてのメディアが [Map Virtual Media CD/ISO Image] (仮想メディア CD/ISO イメージの割り当て) ダイアログ ボックスで選択できるようになりました。

注: LX、KX、KSX、または KX101 G2 デバイスで使用されるサードパーティ ソフトウェアの技術的な制限により、IPv6 アドレスを使用して仮想メディア経由でリモート ISO イメージにアクセスすることはできません。

注:Windows 2003® サーバに接続し、サーバから ISO イメージをロードしようとすると、「Virtual Media mounting on port failed. Unable to connect to the file server or incorrect File Server username and password」(ポートで仮想メディアのマウントに失敗しました。ファイル サーバに接続できないか、ファイル サーバのユーザ名とパスワードが正しくありません）というエラーが表示される場合があります。このエラーが発生した場合は、[Microsoft ネットワーク サーバー: 通信にデジタル署名を行う] オプションを無効にします。

仮想メディアへの接続

[Local Drives] (ローカル ドライブ)

このオプションを使用すると、ドライブ全体がマウントされます。つまり、クライアントコンピュータのディスク ドライブ全体がターゲットサーバに仮想的にマウントされます。このオプションは、ハード ディスク ドライブと外部ドライブにのみ使用してください。ネットワーク ドライブ、CD-ROM ドライブ、または DVD-ROM ドライブは対象外です。これは、[Read/Write] (読み取り/書き込み可能) を指定できる唯一のオプションです。

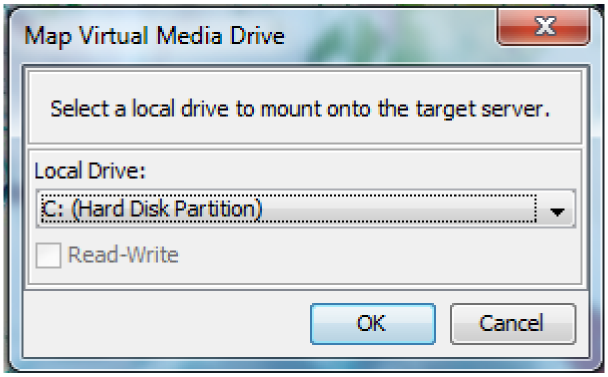
注: Windows XP® オペレーティング システムが稼動している KVM ターゲット サーバでは、NTFS 形式のパーティション (ローカル C ドライブなど) がリダイレクトされた後で新しいマス ストレージ接続を行うことができない場合があります。

その場合には、リモート コンソールを閉じて再接続した後で、別の仮想メディア デバイスをリダイレクトしてください。同じターゲット サーバに別のユーザーが接続している場合、そのユーザーの接続も閉じる必要があります。

注: KX II 2.1.0 (以降) では、フロッピー ディスクなどの外部ドライブをマウントすると、ドライブの LED ライトが点灯したままになります。これは、デバイスが 500 ミリ秒ごとにドライブをチェックして、ドライブがまだマウントされているかどうかを確認するからです。

▶ **クライアント コンピュータの仮想メディア ドライブにアクセスするには、以下の手順に従います。**

1. Virtual KVM Client で、[Virtual Media] (仮想メディア) の [Connect Drive] (ドライブの接続) を選択するか、[Connect Drive...] (ドライブの接続...) ボタン をクリックします。[Map Virtual Media Drive] (仮想メディア ドライブの割り当て) ダイアログ ボックスが表示されます。



2. [Local Drive] (ローカル ドライブ) ドロップダウン リストから、ドライブを選択します。

   読み取りと書き込みの機能が必要な場合には、[Read-Write] (読み取り/書き込み可能) チェックボックスをオンにします。

   このオプションは、リムーバブル ドライブ以外では無効になっています。詳細は、「読み取り/書き込み可能に設定できない状況」を参照してください。

   このチェックボックスをオンにすると、接続した USB ディスクに読み取りと書き込みを実行できるようになります。

   警告: 読み取り/書き込みアクセスを有効にすると危険な場合があります。同じドライブに対して同時に複数のクライアント PC からアクセスすると、データが壊れる恐れがあります。書き込みアクセスが不要な場合は、このオプションをオフのままにしてください。

3. [OK] をクリックします。メディアがターゲット サーバに仮想的にマウントされます。このメディアには、他のドライブとまったく同じようにアクセスすることができます。

読み取り/書き込み可能に設定できない状況

以下の場合、仮想メディアを読み取り/書き込み可能にすることはできません。

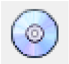
- Linux® および Mac® の各クライアント
- 複数のハード ディスク ドライブすべてが対象の場合
- ドライブが書き込み保護されている場合
- ユーザに読み取り/書き込みの権限がない場合。
  - ポート権限の [Access] (アクセス) が [None] (なし) または [View] (表示) に設定されている場合。
  - ポート権限の [VM Access] (VM アクセス) が [Read-Only] (読み取り専用) または [Deny] (拒否) に設定されている場合。

CD-ROM/DVD-ROM/ISO イメージ

このオプションを使用して、CD-ROM、DVD-ROM、ISO イメージをマウントします。

注:Raritan は ISO9660 形式を標準でサポートしています。ただし、その他の CD-ROM 拡張でも動作します。

▶ CD-ROM、DVD-ROM、ISO イメージにアクセスするには、以下の手順に従います。

1. Virtual KVM Client で、[Virtual Media] (仮想メディア) の [Connect CD-ROM/ISO Image] (CD-ROM/ISO イメージに接続) を選択するか、[Connect CD-ROM/ISO] (CD-ROM/ISO に接続) ボタン  をクリックします。[Map Virtual Media CD/ISO Image] (仮想メディア CD/ISO イメージの割り当て) ダイアログ ボックスが表示されます。
2. 内部および外部の CD-ROM ドライブまたは DVD-ROM ドライブの場合
    a. [Local CD/DVD Drive] (ローカル CD/DVD ドライブ) を選択します。
    b. [Local CD/DVD Drive] (ローカル CD/DVD ドライブ) ドロップダウン リストから、ドライブを選択します。使用可能なすべての内部/外部の CD ドライブおよび DVD ドライブの名前が、ドロップダウン リストに表示されます。
    c. [接続] をクリックします。
3. ISO イメージの場合
    a. [ISO Image] (ISO イメージ) オプションを選択します。CD、DVD、またはハード ディスクのディスク イメージにアクセスする場合に、このオプションを使用します。サポートされる形式は ISO 形式のみです。
    b. [Browse] (参照) をクリックします。
    c. 使用するディスク イメージが含まれるパスを指定して、[Open] (開く) をクリックします。パスが [Image Path] (イメージのパス) フィールドに入力されます。
    d. [接続] をクリックします。
4. ファイル サーバ上のリモート ISO イメージの場合
    a. [Remote Server ISO Image] (リモート サーバの ISO イメージ) オプションを選択します。
    b. ドロップダウン リストから、ホスト名とイメージを選択します。ファイル サーバとイメージ パスは、[File Server Setup] (ファイル サーバのセットアップ) ページを使用して設定できます。[File Server Setup] (ファイル サーバのセットアップ) ページで設定した項目がドロップダウン リストに表示されます。

c. [File Server Username] (ファイル サーバ ユーザ名) – ファイル サーバへのアクセスに必要なユーザ名です。名前には、mydomain/username のようにドメイン名を含めることができます。
d. [File Server Password] (ファイル サーバ パスワード) – ファイル サーバへのアクセスに必要なパスワードです (入力時、フィールドはマスクされます)。
e. [接続] をクリックします。

メディアがターゲット サーバに仮想的にマウントされます。このメディアには、他のドライブとまったく同じようにアクセスすることができます。

注:Linux® ターゲット上のファイルを操作する場合、仮想メディアを使用してコピーしたファイルを表示するには、コピー後に Linux の Sync コマンドを使用します。Sync コマンドを実行するまではファイルを表示できません。

注:Windows 7® オペレーティング システム® を使用している場合、デフォルトでは、ローカル CD/DVD ドライブまたはリモート ISO イメージをマウントしたとき、リムーバブル ディスクは Windows の [マイ コンピュータ] フォルダに表示されません。ローカル CD/DVD ドライブまたはリモート ISO イメージをこのフォルダに表示するには、[ツール] メニューの [フォルダ オプション] をクリックし、[空のドライブは [コンピュータ] フォルダに表示しない] チェック ボックスをオフにします。

注: サードパーティ ソフトウェアの技術的な制限により、IPv6 アドレスを使用して仮想メディア経由でリモート ISO イメージにアクセスすることはできません。

仮想メディアの切断

▶ 仮想メディア ドライブを切断するには、以下の手順に従います。

- ローカル ドライブの場合は、[Virtual Media] (仮想メディア) の [Disconnect Drive] (ドライブの切断) を選択します。
- CD-ROM、DVD-ROM、ISO イメージの場合は、[Virtual Media] (仮想メディア) の [Disconnect CD-ROM/ISO Image] (CD-ROM/ISO イメージの切断) を選択します。

注: 切断コマンドを使用する方法だけでなく、KVM 接続を閉じても仮想メディアが切断されます。

Ch 6 USB プロファイル

この章の内容

概要 115
CIM の互換性.......... 116
使用できる USB プロファイル 116
KVM ポート用のプロファイルの選択 123

概要

さまざまな KVM ターゲット サーバと KSX II との互換性を高めるために、ラリタンは、幅広いオペレーティング システムおよび BIOS レベルのサーバ実装に対応する USB 設定プロファイルの標準的な選択肢を提供しています。

Generic (デフォルト) USB プロファイルは、展開された KVM ターゲット サーバ設定の大部分のニーズを満たしています。

その他のプロファイルは、一般的に展開される他のサーバ設定（例: Linux® や Mac OS X®）の特定のニーズを満たすように提供されています。

たとえば BIOS レベルで実行される場合に、ターゲット サーバとの仮想メディア機能の互換性を強化するための、(プラットフォーム名および BIOS のリビジョンによって指定された) プロファイルも多数あります。

USB プロファイルは、KSX II リモート コンソールおよびローカル コンソールで、[Device Settings] (デバイス設定)、[Port Configuration] (ポート設定)、[Port] (ポート) ページの順に選択して設定します。

管理者は、ユーザおよびターゲット サーバの設定のニーズに最適な USB プロファイルでポートを設定します。

KVM ターゲット サーバに接続するユーザは、KVM ターゲット サーバの動作状態に応じて、*Virtual KVM Client* 『*61*p. の" *Virtual KVM Client (VKC)*"参照 』 で、これらの設定済みのプロファイルの中から選択します。

たとえば、サーバで Windows® オペレーティング システムが実行されている場合は、Generic プロファイルが最適です。

BIOS メニューの設定の変更または仮想メディア ドライブからの起動を行う場合は、ターゲット サーバ モデルによっては、BIOS プロファイルの方が適している可能性があります。

特定の KVM ターゲットで、ラリタンが提供する標準 USB プロファイルがいずれも適切に機能しない場合は、ラリタン テクニカル サポートにお問い合わせください。

CIM の互換性

USB プロファイルを使用するには、ファームウェアが最新であるデジタル CIM、D2CIM-VUSB、または D2CIM-DVUSB を使用する必要があります。ファームウェアを更新していない VM-CIM は、幅広い設定（キーボード、マウス、CD-ROM、およびリムーバブル ドライブ）をサポートしますが、特定のターゲット設定用に最適化されたプロファイルを使用することはできません。この場合に、USB プロファイルにアクセスするためには、既存の VM-CIM を最新のファームウェアでアップグレードする必要があります。なお、アップグレードする前でも、"Generic" プロファイルに相当する機能は利用できます。

VM-CIM ファームウェアは、ファームウェアの更新中に自動的にアップグレードされますが、ファームウェアをアップグレードしていない VM-CIM は、次のページの説明に従ってアップグレードできます。 *CIM をアップグレードする* 『*234*p. の"*CIM アップグレード*"参照 』

詳細は、「*コンピュータ インタフェース モジュール (CIM) の仕様* 『*302*p. の"*コンピュータ インタフェース モジュール (CIM)*"参照 』」を参照してください。

使用できる USB プロファイル

現在のリリースの KSX II には、次の表に示した USB プロファイルが用意されています。新しいプロファイルは、Raritan が提供する各ファームウェア アップグレードに含まれています。新しいプロファイルが追加されると、それがヘルプに記載されます。

USB プロファイル	説明
BIOS Dell® PowerEdge® 1950/2950/2970/6950/R200	Dell PowerEdge 1950/2950/2970/6950/R200 BIOS Dell PowerEdge 1950/2950/2970/6950/R200 BIOS には、このプロファイルまたは 'Generic' プロファイルを使用します。 制限: ▪ なし
BIOS Dell OptiPlex ™ キーボードおよびマウスのみ	Dell OptiPlex BIOS アクセス (キーボードおよびマウスのみ) D2CIM-VUSB を使用している場合に、このプロファイルを使用して、Dell OptiPlex BIOS のキーボード機能を持たせます。新しい D2CIM-DVUSB を使用する場合は、'Generic' プロファイルを使用します。 注意: ▪ Optiplex 210L/280/745/GX620 では、仮想メディアをサポートするために、D2CIM-DVUSB を 'Generic' プロファイルで使用する必要があります。

USB プロファイル	説明
	制限: ▪ USB バス速度はフルスピード (12 MBit/s) に制限されます。 ▪ 仮想メディアはサポートされていません。
BIOS Dell Optiplex 790	BIOS 操作中は、Dell Optiplex 790 にこのプロファイルを使用します。 警告: ▪ USB の列挙は、仮想メディアが接続または切断されるときに開始されます。 制限: ▪ USB バス速度はフルスピード (12 MBit/s) に制限されます。 ▪ ずれないマウスはサポートされていません。 ▪ 仮想 CD-ROM およびディスク ドライブを同時に使用することはできません。
BIOS Dell Optiplex 790 キーボードのみ	BIOS 操作中、キーボード マクロを使用するときに、Dell Optiplex 790 にこのプロファイルを使用します。このプロファイルでは、キーボードのみが有効になります。 制限: ▪ マウスは無効になります。 ▪ 仮想 CD-ROM およびディスク ドライブは無効になります。

USB プロファイル	説明
BIOS DellPowerEdge キーボードおよびマウスのみ	Dell PowerEdge BIOS アクセス (キーボードおよびマウスのみ) D2CIM-VUSB を使用している場合に、このプロファイルを使用して、Dell PowerEdge BIOS のキーボード機能を持たせます。新しい D2CIM-DVUSB を使用する場合は、'Generic' プロファイルを使用します。 注意: ▪ PowerEdge 650/1650/1750/2600/2650 BIOS では、USB CD-ROM およびディスク ドライブは起動可能デバイスとしてはサポートされていません。 ▪ PowerEdge 750/850/860/1850/2850/SC1425 BIOS で仮想メディアをサポートするには、D2CIM-DVUSB を 'Generic' プロファイルで使用する必要があります。 ▪ BIOS で実行している場合は、PowerEdge 1950/2950/2970/6950/R200 に 'BIOS Dell PowerEdge 1950/2950/2970/6950/R200' または 'Generic' プロファイルを使用します。 制限: ▪ USB バス速度はフルスピード (12 MBit/s) に制限されます。 ▪ ずれないマウス (Absolute mouse synchronization™) はサポートされていません。 ▪ 仮想メディアはサポートされていません。
BIOS ASUS P4C800 マザーボード	BIOS にアクセスしたり、Asus P4C800 ベースのシステムで仮想メディアから起動したりするには、このプロファイルを使用します。 制限: ▪ USB バス速度はフルスピード (12 MBit/s) に制限されます。 ▪ 仮想 CD-ROM およびディスク ドライブを同時に使用することはできません。

USB プロファイル	説明
BIOS 汎用	BIOS 汎用 このプロファイルは Generic OS プロファイルが BIOS で機能しない場合に使用します。 警告: USB の列挙は、仮想メディアが接続または切断されるときに開始されます。 制限: ▪ USB バス速度はフルスピード (12 MBit/s) に制限されます。 ▪ ずれないマウス (Absolute mouse synchronization™) はサポートされていません。 ▪ 仮想 CD-ROM およびディスク ドライブを同時に使用することはできません。
BIOS HP® Proliant™ DL145	HP Proliant DL145 PhoenixBIOS HP Proliant DL145 PhoenixBIOS では、OS のインストール中に、このプロファイルを使用します。 制限: ▪ USB バス速度はフルスピード (12 MBit/s) に制限されます。
BIOS HP Compaq® DC7100/DC7600	BIOS HP Compaq DC7100/DC7600 HP Compaq DC7100/DC7600 シリーズのデスクトップを仮想メディアから起動するにはこのプロファイルを使用します。 制限: ▪ 仮想 CD-ROM およびディスク ドライブを同時に使用することはできません。
BIOS IBM ThinkCentre Lenovo	IBM Thinkcentre Lenovo BIOS BIOS 操作中は IBM® Thinkcentre Lenovo システム ボード (828841U モデル) にこのプロファイルを使用します。 制限: ▪ USB バス速度はフルスピード (12 MBit/s) に制限されます。 ▪ 仮想 CD-ROM およびディスク ドライブを同時に使用することはできません。
アドバンスト マネージメント モジュールを装備した IBM BladeCenter H	D2CIM-VUSB または D2CIM-DVUSB がアドバンスト マネージメント モジュールに接続されている場合に、仮想メディア機能を有効にするには、このプロファイルを使用します。 制限: ▪ 仮想 CD-ROM およびディスク ドライブを同時に使用することはできません。

USB プロファイル	説明
BIOS Lenovo ThinkPad T61 & X61	BIOS Lenovo ThinkPad T61 および X61 (仮想メディアから起動) T61 および X61 シリーズのラップトップを仮想メディアから起動するには、このプロファイルを使用します。 制限: ▪ USB バス速度はフルスピード (12 MBit/s) に制限されます。
Generic (汎用)	汎用 USB プロファイルは、オリジナルの リリースの動作と似ています。このプロファイルは、Windows 2000®、Windows XP®、Windows Vista®、およびそれ以降の Windows に対して使用します。 制限: ▪ なし
HP Proliant DL360/DL380 G4 (HP SmartStart CD)	HP Proliant DL360/DL380 G4 (HP SmartStart CD) このプロファイルは、HP Proliant DL360/DL380 G4 シリーズのサーバで HP SmartStart CD を使用して OS をインストールする場合に使用します。 制限: ▪ USB バス速度はフルスピード (12 MBit/s) に制限されます。 ▪ ずれないマウス (Absolute mouse synchronization™) はサポートされていません。
HP Proliant DL360/DL380 G4 (Windows® Server 2003 インストール)	HP Proliant DL360/DL380 G4 (Windows Server 2003 インストール) このプロファイルは、HP Proliant DL360/DL380 G4 シリーズのサーバで HP SmartStart CD を使用せずに Windows Server 2003 をインストールする場合に使用します。 制限: ▪ USB バス速度はフルスピード (12 MBit/s) に制限されます。
Linux®	汎用 Linux プロファイル これは、汎用 Linux プロファイルです。Redhat Enterprise Linux、SuSE Linux Enterprise Desktop、および類似のディストリビューションで使用されます。 制限: ▪ ずれないマウス (Absolute mouse synchronization™) はサポートされていません。
BIOS Mac®	BIOS Mac このプロファイルは Mac BIOS に使用します。 制限: ▪ ずれないマウス (Absolute mouse synchronization™) はサポートされていません。

USB プロファイル	説明
	■ 仮想 CD-ROM およびディスク ドライブを同時に使用することはできません。 この USB プロファイルを使用する場合、Mac のブート メニューを使用するときのマウス モードについては、「*Mac のブート メニュー使用時のマウス モード*『*123*p. 』」を参照してください。
MAC OS X® 10.4.9 (以降)	MAC OS X バージョン 10.4.9 (以降) このプロファイルは、最近のバージョンの Mac OS X で導入されたマウス座標のスケーリングを補正します。リモートおよびローカルのマウスの位置がデスクトップの境界の近くで同期しない場合はこれを選択します。 制限: ■ 仮想 CD-ROM およびディスク ドライブを同時に使用することはできません。
RUBY 工業用メインボード (AwardBIOS)	RUBY 工業用メインボード (AwardBIOS) このプロファイルは、Phoenix/AwardBIOS v6.00PG を使用する RUBY-9715VG2A シリーズの工業用メインボードで使用します。 制限: ■ USB バス速度はフルスピード (12 MBit/s) に制限されます。 ■ 仮想 CD-ROM およびディスク ドライブを同時に使用することはできません。
Supermicro Mainboard Phoenix (AwardBIOS)	Supermicro メインボード Phoenix (AwardBIOS) このプロファイルは、Phoenix AwardBIOS を使用する Supermicro シリーズのメインボードで使用されます。 制限: ■ 仮想 CD-ROM およびディスク ドライブを同時に使用することはできません。
Suse 9.2	SuSE Linux 9.2 これは SuSE Linux 9.2 ディストリビューションで使用されます。 制限: ■ ずれないマウス (Absolute mouse synchronization™) はサポートされていません。 ■ USB バス速度はフルスピード (12 MBit/s) に制限されます。
Troubleshooting 1	トラブルシューティング プロファイル 1 ■ マス ストレージが優先 ■ キーボードおよびマウス (タイプ 1) ■ USB バス速度はフルスピード (12 MBit/s) に制限されます。 ■ 仮想 CD-ROM およびディスク ドライブを同時に使用するこ

USB プロファイル	説明
	とはできません。 警告: USB の列挙は、仮想メディアが接続または切断されるときに開始されます。
Troubleshooting 2	トラブルシューティング プロファイル 2 ▪ キーボードおよびマウス（タイプ 2）優先 ▪ マス ストレージ ▪ USB バス速度はフルスピード（12 MBit/s）に制限されます。 ▪ 仮想 CD-ROM およびディスク ドライブを同時に使用することはできません。 警告: USB の列挙は、仮想メディアが接続または切断されるときに開始されます。
Troubleshooting 3	トラブルシューティング プロファイル 3 ▪ マス ストレージが優先 ▪ キーボードおよびマウス（タイプ 2） ▪ USB バス速度はフルスピード（12 MBit/s）に制限されます。 ▪ 仮想 CD-ROM およびディスク ドライブを同時に使用することはできません。 警告: USB の列挙は、仮想メディアが接続または切断されるときに開始されます。
仮想メディア CIM でフルスピードを使用	仮想メディア CIM でフルスピードを使用 このプロファイルは、[Full Speed for Virtual Media CIM]（仮想メディア CIM でフルスピードを使用）オプションを選択したオリジナルの リリースの動作に似ています。高速 USB デバイスを処理できない BIOS に便利です。 制限: ▪ USB バス速度はフルスピード（12 MBit/s）に制限されます。
キーボードおよびマウスの USB でフル スピードを使用	このプロファイルでは、デュアル VM CIM のキーボードおよびマウスの USB インタフェースがフル スピードに設定されます。低速 USB 設定では正しく動作できないデバイスに有効です。 制限: ▪ キーボードおよびマウスの USB インタフェースの USB バス速度は、フル スピード（12 MBit/s）に設定されます。

KVM ポート用のプロファイルの選択

KSX II には、USB プロファイルのセットが含まれているので、接続先の KVM ターゲット サーバの特性に基づいて KVM ポートを割り当てることができます。KSX II リモートまたはローカル コンソールで、[Device Settings] (デバイス設定)、[Port Configuration] (ポート設定)、[Port] (ポート) ページの順に選択し、USB プロファイルを KVM ポートに割り当てています。

特定のターゲットで必要になる可能性が最も高いプロファイルを指定するのは、管理者です。これらのプロファイルは、MPC、AKC、および VKC 経由での選択に使用できるようになります。プロファイルを利用できない場合は、[USB Profile] (USB プロファイル) の [Other Profiles] (他のプロファイル) を選択して、使用可能なプロファイルにアクセスできます。

USB プロファイルを KVM ポートに割り当てると、ユーザが KVM ターゲット サーバに接続するときにそれらのプロファイルを使用できるようになります。必要な場合は、VKC、AKC、または MPC の [USB Profile] (USB プロファイル) メニューから USB プロファイルを選択できます。

USB プロファイルを KVM ポートに割り当てる方法の詳細は、「*USB プロファイルの設定 ([Port] (ポート) ページ)* 『*199*p. 』」を参照してください。

Mac のブート メニュー使用時のマウス モード

USB プロファイルの使用時に、Mac のブート メニューでマウスを使用するには、ずれないマウス モードが BIOS でサポートされていないので、シングル マウス モードにする必要があります。

▶ **ブート メニューで動作するようにマウスを設定するには、以下の手順に従います。**

1. Mac を再起動し、再起動中に option キーを押してブート メニューを開きます。この時点では、マウスは応答しません。
2. シングル マウス モードを選択します。これで、マウスが応答します。

   注:シングル マウス モードでは、マウスの速度が遅くなることがあります。

3. ブート メニューから OS X に戻る場合は、シングル マウス モードを終了し、ずれないマウス モードに切り替えます。

Ch 7　User Management

この章の内容

ユーザ グループ.. 124
ユーザ.. 132
[Authentication Settings] (認証設定).. 134
パスワードの変更.. 146

ユーザ グループ

KSX II は、アクセスの認可と許可を決定するためにユーザ名とグループ名の内部リストを保持しています。この情報は、暗号化形式で内部に保存されます。認証にはいくつかの方式があり、この方式は「ローカル認証」と呼ばれます。すべてのユーザは認証を受ける必要があります。LDAP/LDAPS または RADIUS 認証を行うように KSX II が設定されている場合、その認証が行われた後に、ローカル認証が行われます。

すべての KSX II には、3 つのデフォルト ユーザ グループが存在します。これらのグループは削除できません。

ユーザ	説明
[Admin] (管理)	このグループに所属するユーザは、完全な管理者特権を持ちます。元の製品出荷時のデフォルト ユーザはこのグループのメンバーであり、完全なシステム特権を持ちます。さらに、Admin (管理者) ユーザは Admin (管理者) グループのメンバーである必要があります。
Unknown (不明)	LDAP/LDAPS または RADIUS を使用して外部的に認証されるユーザまたはシステムで既知のユーザのデフォルト グループです。外部 LDAP/LDAPS サーバまたは RADIUS サーバによって有効なユーザ グループが識別されなかった場合、Unknown (不明) グループが使用されます。さらに、新規に作成されたユーザは別のグループに割り当てられるまでこのグループに自動的に配置されます。
Individual Group (個別グループ)	個別グループとは、基本的に個人の「グループ」です。つまり、特定のユーザは独自のグループに属し、他の実際のグループには属しません。個別グループは、グループ名の先頭に "@" が付けられているので区別できます。個別グループでは、グループと同じ権限をユーザ アカウントに割り当てることができます。

KSX II 内では最大 254 個のユーザ グループを作成できます。

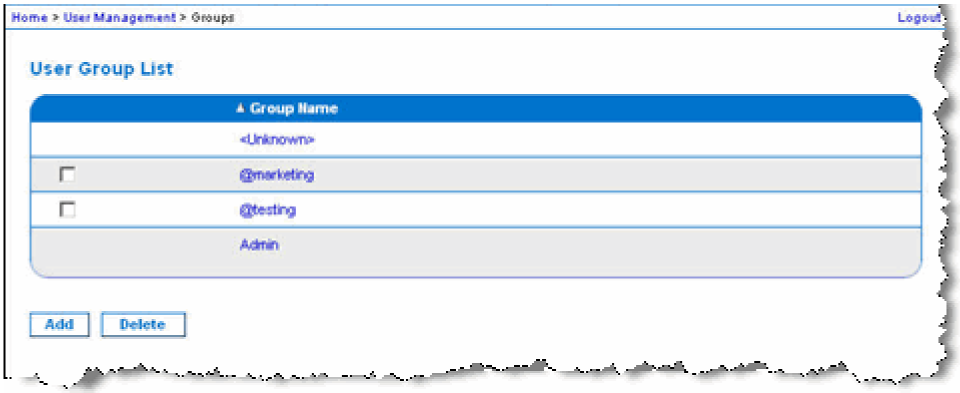
ユーザ グループ リスト

ユーザ グループは、ローカル認証とリモート認証（RADIUS または LDAP/LDAPS）で使用されます。個別のユーザを作成する場合は、事前にユーザ グループを定義しておいてください。それは、ユーザを追加するときに、ユーザを既存のユーザ グループに割り当てる必要があるからです。

［ユーザ グループ リスト］ページには、すべてのユーザ グループのリストが表示されます。このリストは、［グループ名］列見出しをクリックすることで、昇順または降順に並べ替えることができます。［ユーザ グループ リスト］ページでは、ユーザ グループを追加、変更、または削除することもできます。

▶ ユーザ グループのリストを表示するには、以下の手順に従います。

- ［ユーザ管理］の［ユーザ グループ リスト］を選択します。［ユーザ グループ リスト］ページが開きます。



ユーザとグループの関係

ユーザはグループに属し、グループには特権が割り当てられています。KSX II の各種のユーザをグループに分けることにより、ユーザごとに許可を管理する必要がなくなり、あるグループ内のすべてユーザの許可を一度に管理できるようになるので、時間の節約につながります。

また、特定のユーザをグループに割り当てないようにすることも可能です。その場合は、ユーザを「個別」として分類します。

認証が成功すると、デバイスは、グループ情報を使用して、アクセスできるサーバ ポート、デバイスの再起動を許可するかどうかなど、そのユーザの許可を決定します。

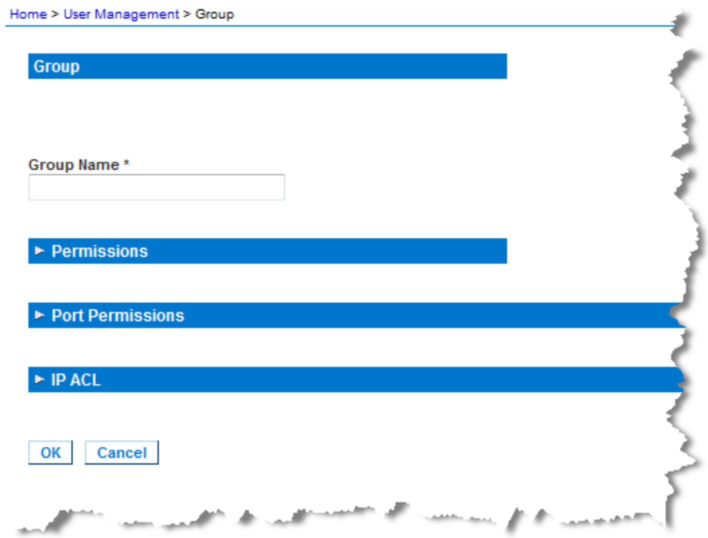
新規ユーザ グループの追加

▶ 新規ユーザ グループを追加するには、以下の手順に従います。

1. [User Management] (ユーザ管理) の [Add New User Group] (新規ユーザ グループの追加) を選択するか、[User Group List] (ユーザ グループ リスト) ページの [Add] (追加) をクリックします。
2. [Group Name] (グループ名) フィールドに、新しいユーザ グループのわかりやすい名前 (最大 64 文字) を入力します。
3. このグループに属するすべてのユーザに対して割り当てる許可の横にあるチェックボックスをオンにします。「許可の設定」を参照してください。「***権限*** 『*127*p. 』」を参照してください。
4. このグループに属するユーザがアクセスできるサーバ ポートと、そのアクセスのタイプを指定します。「ポート権限の設定」を参照してください。「***ポート権限*** 『*128*p. 』」を参照してください。
5. 「IP ACL を設定します。この機能は、IP アドレスを指定することで、KSX II デバイスへのアクセスを制限します。この機能は、特定のグループに属するユーザにのみ適用されます。このデバイスに対するすべてのアクセス試行に適用され、優先される、IP アクセス制御リスト機能とは異なります。「グループベースの IP ACL (アクセス制御リスト)」を参照してください。***グループベースの IP ACL (アクセス制御リスト)*** 『*129*p. 』」を参照してください。
6. [OK] をクリックします。

注: 複数の管理機能を MPC 内および KSX II ローカル コンソールから利用できます。これらの機能を利用できるのは、デフォルトの Admin (管理者) グループのメンバーに限られます。

注: IPv4 と IPv6 の両方のアドレスがサポートされています。



個別グループの許可の設定

▶ **個別ユーザ グループに許可を設定するには、以下の手順に従います。**

1. グループ リストから目的のグループを探します。個別グループは、グループ名の先頭に @ が付けられているので区別できます。
2. グループ名をクリックします。[Group] (グループ) ページが開きます。
3. 適切な許可を選択します。
4. [OK] をクリックします。

権限

重要: [User Management] (ユーザ管理) チェックボックスをオンにすると、グループのメンバーは、自身も含むすべてのユーザの許可を変更することができます。これらの許可を付与する場合は注意してください。

許可	説明
[Device Access While Under CC-SG Management] (CC-SG 管理下のデバイス アクセス)	この許可を持つユーザとユーザ グループは、CC-SG のデバイスに対してローカル アクセスが有効になっている場合に IP アドレスを使用して直接 KSX II にアクセスできます。デバイスには、ローカル コンソール、リモート コンソール、MPC、VKC、および AKC からアクセスできます。 CC-SG の管理下にあるデバイスに直接アクセスすると、KSX II でアクセスおよび接続アクティビティがログに記録されます。ユーザ認証は、KSX II の認証設定に基づいて実行されます。 *注: 管理者ユーザ グループには、この許可がデフォルトで付与されます。*
[Device Settings] (デバイス設定)	ネットワーク設定、日付/時刻設定、ポート設定 (チャンネル名、電源の関連付け)、イベント管理 (SNMP、Syslog)、仮想メディア ファイル サーバのセットアップ
診断	ネットワーク インタフェース ステータス、ネットワーク統計、ホストへの Ping、ホストへのトレース ルート、KSX II 診断
保守	データベースのバックアップとリストア、ファームウェアのアップグレード、ファクトリ リセット、再起動

許可	説明
[Modem Access] (モデム アクセス)	モデムを使用して KSX II デバイスに接続する許可
[PC-Share] (PC 共有)	複数のユーザによる同一ターゲットへの同時アクセス
セキュリティ	SSL 証明書、セキュリティ設定 (VM 共有、PC 共有)、IP ACL
[User Management] (ユーザ管理)	ユーザおよびグループの管理、リモート認証 (LDAP/LDAPS/RADIUS)、ログイン設定

ポート権限

それぞれのサーバ ポートに対して、そのグループが持つアクセスのタイプ、仮想メディアへのポート アクセスのタイプ、および電源管理を指定できます。すべての権限についてデフォルト設定はすべて [Deny] (拒否) になっていることに注意してください。

ポート アクセス オプションです。	説明
[Deny] (拒否)	アクセスを完全に拒否します。
[View] (表示)	接続先のターゲット サーバのビデオを表示します (操作はできません)。
[Control] (制御)	接続先のターゲット サーバを制御します。VM および電源管理アクセスも付与される場合は、[Control] (制御) を割り当てる必要があります。

VM アクセス オプション	説明
[Deny] (拒否)	ポートに対して仮想メディア許可はすべて拒否されます。
[Read-Only] (読み取り専	仮想メディア アクセスは、読み取りアクセスのみに制限されます。

VM アクセス	
用)	
[Read-Write] (読み取り/書き込み可能)	仮想メディアに対する完全なアクセス（読み取り、書き込み）が許可されます。

電源管理アクセス

オプション	**説明**
[Deny] (拒否)	ターゲット サーバに対する電源管理を拒否します。
[Access] (アクセス)	ターゲット サーバでの電源管理を完全に許可します。

ブレード シャーシの場合、ポート アクセス権限によって、そのブレード シャーシに設定されている URL へのアクセスを制御します。オプションは、[Deny] (拒否) または [Control] (制御) です。また、シャーシ内の各ブレードには、固有の独立ポート権限設定があります。

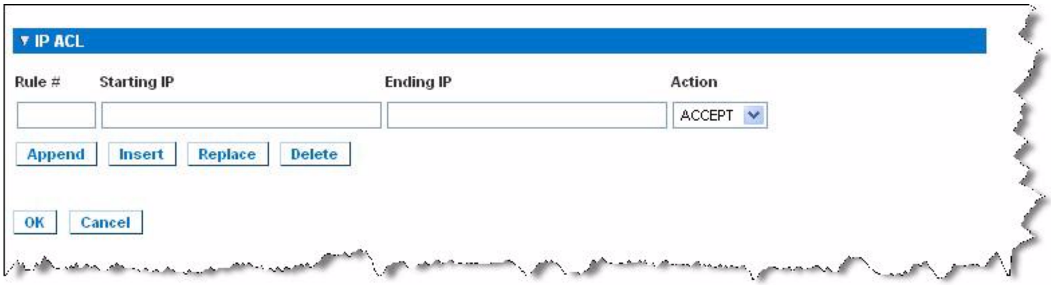
グループベースの IP ACL (アクセス制御リスト)

重要: グループベースの IP アクセス制御を使用する場合は注意が必要です。アクセスが拒否されている IP アドレスの範囲に自分の IP アドレスが含まれている場合、KSX II がロックアウトされてしまいます。

この機能は、選択したグループに含まれるユーザによる KSX II デバイスへのアクセスを特定の IP アドレスに制限します。この機能は、デバイスへのすべてのアクセス試行に適用される（および最初に処理され、優先される）IP アクセス制御リスト機能とは異なり、特定のグループに属するユーザにのみ適用されます。

重要: KSX II ローカル ポートでは、IP アドレス 127.0.0.1 が使用され、ブロックはできません。

グループレベルで IP アクセス制御ルールの追加、挿入、置換、削除を行うには、[Group] (グループ) ページの [IP ACL] (IP ACL) セクションを使用します。



▶ ルールを一覧の末尾に追加するには

1. [Starting IP] (開始 IP) フィールドに、開始 IP アドレスを入力します。
2. [Ending IP] (終了 IP) フィールドに、終了 IP アドレスを入力します。
3. 利用可能なオプションからアクションを選択します。
   - [Accept] (承諾) – その IP アドレスによる KSX II デバイスへのアクセスが許可されます。
   - [Drop] (拒否) – その IP アドレスによる KSX II デバイスへのアクセスが拒否されます。
4. [Append] (追加) をクリックします。そのルールがルール一覧の末尾に追加されます。入力する各ルールについて、手順 1 ～ 4 を繰り返します。

▶ ルールを一覧の途中に挿入するには

1. ルール番号 (#) を入力します。[Insert] (挿入) コマンドを使用する際にルール番号が必要です。
2. [Starting IP] (開始 IP) フィールドと [Ending IP] (終了 IP) フィールドに IP アドレスを入力します。
3. [Action] (アクション) ドロップダウン リストからアクションを選択します。
4. [Insert] (挿入) をクリックします。入力したルール番号が既存のルール番号と同じである場合は、新しいルールは既存のルールの上に挿入され、リスト内のすべてのルールが下に下がります。

▶ ルールの内容を置換するには

1. 置き換えるルール番号を指定します。
2. [Starting IP] (開始 IP) フィールドと [Ending IP] (終了 IP) フィールドに IP アドレスを入力します。
3. ドロップダウン リストからアクションを選択します。
4. [Replace] (置換) をクリックします。同じルール番号を持つ元のルールが新しいルールに置き換わります。

▶ ルールを削除するには

1. 削除するルール番号を指定します。
2. [Delete] (削除) をクリックします。
3. 削除を確認するプロンプトが表示されたら、[OK] をクリックします。

重要: ACL のルールは、リスト表示されている順に評価されます。たとえばこの例において、2 つの ACL ルールの順番が逆になると、Dominion は通信を全く受けることができなくなります。

Rule 1, Starting IP = 192.168.50.1, Ending IP = 192.168.55.255, Action = ACCEPT

Rule 2, Starting IP = 0.0.0.0, Ending IP = 255.255.255.255, Action = DROP

ヒント: ルール番号を使用すると、各ルールを作成する順序を気にせずに済みます。

既存のユーザ グループの変更

注:Admin (管理者) グループに対しては、すべての許可が有効になっており、変更はできません。

▶ 既存のユーザ グループを変更するには、以下の手順に従います。

1. [Group] (グループ) ページで、適切なフィールドを変更し、適切な許可を設定します。
2. グループに対する許可を設定します。このグループに属するすべてのユーザに対して割り当てる許可の左にあるチェックボックスをオンにします。「許可の設定」を参照してください。
3. [Port Permissions] (ポート権限) を設定します。このグループに属するユーザがアクセスできるサーバ ポート (およびアクセスのタイプ) を指定します。「ポート権限の設定」を参照してください。
4. IP ACL を設定します (オプション)。この機能は、IP アドレスを指定することで、KSX II デバイスへのアクセスを制限します。「グループベースの IP ACL (アクセス制御リスト)」を参照してください。
5. [OK] (OK) をクリックします。

▶ ユーザ グループを削除するには、以下の手順に従います。

重要: ユーザを含むグループを削除すると、そのユーザは <Unknown (不明)> ユーザ グループに自動的に割り当てられます。

ヒント: 特定のグループに属しているユーザを調べるには、ユーザ グループ別にユーザ リストを並べ替えます。

1. リストのグループ名の左にあるチェックボックスをオンにして、目的のグループを選択します。
2. [Delete] (削除) をクリックします。
3. 削除を確認するプロンプトが表示されたら、[OK] をクリックします。

ユーザ

ユーザが KSX II にアクセスするには、ユーザ名とパスワードを付与されている必要があります。この情報は、KSX II にアクセスしようとしているユーザを認証するために使用されます。

KSX II ユーザ リストの表示

[User List] (ユーザ リスト) ページには、すべてのユーザについて、ユーザ名、フル ネーム、およびユーザ グループが表示されます。このリストは、任意の列名をクリックすることで並べ替えることができます。[User List] (ユーザ リスト) ページでは、ユーザを追加、変更、または削除できます。

各ユーザの接続先ポートを表示するには、「ポート別のユーザの表示」を参照してください。

▶ ユーザ リストを表示するには、以下の手順に従います。

- [User Management] (ユーザ管理) の [User List] (ユーザ リスト) を選択します。[User List] (ユーザ リスト) ページが開きます。

新規ユーザの追加

KSX II ユーザを作成する場合は、事前にユーザ グループを定義しておいてください。それは、ユーザを追加するときに、ユーザを既存のユーザ グループに割り当てる必要があるからです。詳細については、「***新しいユーザ グループの追加***『*126*p. の"***新規ユーザ グループの追加***"参照先 』」を参照してください。

[User] (ユーザ) ページでは、新規ユーザの追加、ユーザ情報の変更、無効化されているユーザの再有効化を行うことができます。

*注: ユーザがログインに失敗した回数が [Security Settings] (セキュリティ設定) ページで設定されているログイン失敗の最大許容回数を超えた場合、そのユーザ名は無効化されます。詳細は、「***セキュリティの設定***『207p. 』」を参照してください。*

▶ 新規ユーザを追加するには、以下の手順に従います。

1. [User Management] (ユーザ管理) の [Add New User] (新規ユーザの追加) を選択するか、[User List] (ユーザ リスト) ページの [Add] (追加) ボタンをクリックして、[User] (ユーザ) ページを開きます。
2. [Username] (ユーザ名) フィールドに、一意のユーザ名を入力します (最大 16 文字)。
3. [Full Name] (フル ネーム) フィールドに、ユーザのフル ネームを入力します (最大 64 文字)。

4. [Password] (パスワード) フィールドにパスワードを入力し、[Confirm Password] (パスワードの確認) フィールドにパスワードを再入力します (最大 64 文字)。
5. ダイヤルバック番号がある場合は、[Dialback Number] (ダイヤルバック番号) フィールドに入力します。ダイヤルバック番号には、以下の文字を含めることはできません。含まれていると、ログインは失敗します。
   - ″ 二重引用符
   - ' 一重引用符
   - ; セミコロン
   - $ ドル記号
   - & アンパサンド
   - ½ パイプ記号
6. [User Group] (ユーザ グループ) ドロップダウン リストからグループを選択します。このリストには、システムによって定義されている デフォルト グループ ([<Unknown>] (不明) (デフォルト設定)、[Admin] (管理者)、[Individual Group] (個別グループ)) に加えて、ユーザによって作成されたグループを含むすべてのグループが表示されます。

   このユーザを既存のユーザ グループに関連付けたくない場合は、ドロップダウン リストから [Individual Group] (個別グループ) を選択します。個別グループの許可についての詳細は、「***個別グループの許可の設定*** 『*127*p. 』」を参照してください。
7. 新規ユーザを有効にするには、[Active] (アクティブ) チェックボックスをオンにします。デフォルトはアクティブ状態 (有効) です。
8. [OK] をクリックします。

既存のユーザ グループの変更

▶ 既存のユーザを変更するには、以下の手順に従います。

1. [User Management] (ユーザ管理) の [User List] (ユーザ リスト) を選択して、[User List] (ユーザ リスト) ページを開きます。
2. [User List] (ユーザ リスト) ページのリストから目的のユーザを探します。
3. ユーザ名をクリックします。[User] (ユーザ) ページが開きます。
4. [User] (ユーザ) ページで、目的のフィールドを変更します [User] (ユーザ) ページにアクセスする方法についての詳細は、「新規ユーザの追加」を参照してください。
5. ユーザを削除するには、[Delete] (削除) をクリックします。削除してよいかどうかを確認するダイアログ ボックスが開きます。
6. [OK] (OK) をクリックします。

KSX II からのユーザのログオフ (強制ログオフ)

管理者である場合は、KSX II にログオンしているユーザのうち、認証されているユーザをログオフすることができます。また、ユーザをポートレベルでポートから切断することもできます。「ポートからのユーザの切断」を参照してください。

▶ **ユーザを KSX II からログオフするには、以下の手順に従います。**

1. [User Management] (ユーザ管理) の [Users by Port] (ポート別ユーザ) を選択します。[Users by Port] (ポート別ユーザ) ページが開きます。
2. ターゲットから切断するユーザの名前の横にあるチェックボックスをオンにします。
3. [Force User Logoff] (ユーザの強制ログオフ) をクリックします。
4. [Logoff User] (ユーザのログオフ) の確認メッセージに対して [OK] をクリックします。

[Authentication Settings] (認証設定)

認証とは、ユーザが本物であることを確認するプロセスです。ユーザが認証されると、ユーザの属するグループに基づいて、システムおよびポートに対する許可が決定されます。ユーザに割り当てられた特権により、どのようなタイプのアクセスが許可されるかが決まります。これを「認可」と呼びます。

KSX II がリモート認証用に構成されている場合、外部認証サーバは主に認証を目的として使用され、認可用には使用されません。

[Authentication Settings] (認証設定) ページでは、KSX II へのアクセスに使用する認証の種類を設定できます。

注: リモート認証 (LDAP/LDAPS または RADIUS) を選択すると、ユーザが見つからない場合はローカル認証データベースも確認されます。

▶ **認証を設定するには、以下の手順に従います。**

1. [ユーザ管理] の [認証設定] を選択します。[認証設定] ページが開きます。
2. 使用する認証プロトコルのオプションを選択します ([ローカル認証]、[LDAP/LDAPS]、または [RADIUS])。[LDAP] オプションを選択した場合、LDAP に関連するフィールドが有効になります。[RADIUS] オプションを選択した場合、RADIUS に関連するフィールドが有効になります。
3. [ローカル認証] を選択した場合は、手順 6 に進みます。
4. [LDAP/LDAPS] を選択した場合は、「***LDAP/LDAPS リモート認証の実装*** 『*135*p. 』」を参考にして、[認証設定] ページの [LDAP] セクションの各フィールドを指定してください。

5. [RADIUS] を選択した場合は、「*RADIUS リモート認証の実装*『*140*p. 』」を参考にして、[認証設定] ページの [RADIUS] セクションの各フィールドを指定してください。
6. [OK] をクリックして保存します。

▶ 工場出荷時のデフォルトに戻すには、以下の手順に従います。

- [デフォルトに戻す] をクリックします。

LDAP/LDAPS リモート認証の実装

Lightweight Directory Access Protocol (ライトウェイト ディレクトリ アクセス プロトコル: LDAP/LDAPS) は、TCP/IP 上で動作するディレクトリ サービスを照会および変更するためのネットワーキング プロトコルです。クライアントは、LDAP/LDAPS サーバ (デフォルトの TCP ポートは 389) に接続して、LDAP セッションを開始します。次に、クライアントは、オペレーション要求をサーバに送信します。サーバは、この要求に対して応答を返します。

メモ: Microsoft® Active Directory® は、LDAP/LDAPS 認証サーバとしてネイティブに機能します。

▶ LDAP 認証プロトコルを使用するには、以下の手順に従います。

1. [User Management] (ユーザ管理) の [Authentication Settings] (認証設定) をクリックして、[Authentication Settings] (認証設定) をページを開きます。
2. [LDAP] (LDAP) ラジオ ボタンを選択して、ページの [LDAP] (LDAP) セクションを有効にします。
3.

アイコンをクリックして、ページの [LDAP] (LDAP) セクションを展開します。

サーバの設定

4. [Primary LDAP Server] (プライマリ LDAP サーバ) フィールドに、LDAP/LDAPS リモート認証サーバの IP アドレスまたは DNS 名を入力します (最大 256 文字)。[Enable Secure LDAP] (セキュア LDAP を有効にする) チェックボックスをオンにし、[Enable LDAPS Server Certificate Validation] (LDAPS サーバ証明書の検証を有効にする) チェックボックスをオンにした場合は、LDAP サーバ証明書の CN に一致する DNS 名を使用する必要があります。
5. [Secondary LDAP Server] (セカンダリ LDAP サーバ) フィールドに、バックアップ LDAP/LDAPS サーバの IP アドレスまたは DNS 名を入力します (最大 256 文字)。[Enable Secure LDAP] (セキュア LDAP を有効にする) オプションをオンにした場合は、DNS 名を使用する必要があります。残りのフィールドについては、[Primary LDAP Server] (プライマリ LDAP サーバ) フィールドの場合と同じ設定を使用します。**(オプション)**

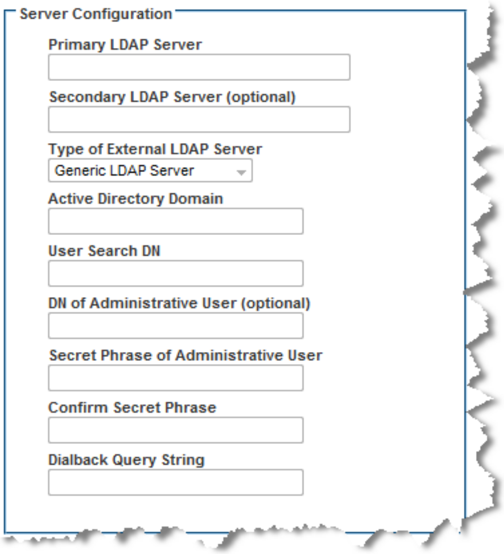
6. [Type of External LDAP Server] (外部 LDAP サーバの種類)。
7. 外部 LDAP/LDAPS サーバを選択します。使用可能なオプションを選択します。
   - [Generic LDAP Server] (一般的な LDAP サーバ)。
   - [Microsoft Active Directory]。Active Directory は、Windows 環境向けの Microsoft による LDAP/LDAPS ディレクトリ サービスの実装です。
8. Microsoft Active Directory を選択した場合は、Active Directory ドメインの名前を入力します。たとえば、*acme.com* などです。特定のドメインの名前については、Active Directive 管理者にお問い合わせください。
9. [User Search DN] (ユーザ検索 DN) フィールドに、LDAP データベース内でユーザ情報の検索を開始する場所の識別名を入力します。最大 64 文字まで使用できます。たとえば、`cn=Users,dc=raritan,dc=com` というベース検索値を設定します。このフィールドに入力する適切な値については、担当の認証サーバ管理者に問い合わせてください。
10. [DN of administrative User] (管理者ユーザの DN) フィールドに管理者ユーザの識別名を入力します (最大 64 文字)。このフィールドは、LDAP サーバで管理者に管理者ユーザの役割を使用したユーザ情報の検索を許可している場合にのみ入力します。このフィールドに入力する適切な値については、担当の認証サーバ管理者に問い合わせてください。たとえば、管理者ユーザの DN として、以下のように設定します。

    `cn=Administrator,cn=Users,dc=testradius,dc=com`**(オプション)**
11. [Dialback Query String] (ダイヤルバック クエリ文字列) フィールドに、ダイヤルバック クエリ文字列を入力します。**(オプション)**

    Microsoft Active Directory を使用している場合は、以下の文字列を入力する必要があります。msRADIUSCallbackNumberMicrosoft Active Directory を使用しない場合は、LDAP サーバに対して定義されている属性文字列を使用します。

    注: この文字列では大文字と小文字が区別されます。

12. 管理者ユーザの識別名を入力した場合は、管理者ユーザの DN をリモート認証サーバに対して認証するために使用するパスワードを入力する必要があります。[Secret Phrase] (秘密フレーズ) フィールドにパスワードを入力し、[Confirm Secret Phrase] (秘密フレーズの確認) フィールドにパスワードを再入力します (最大 128 文字)。

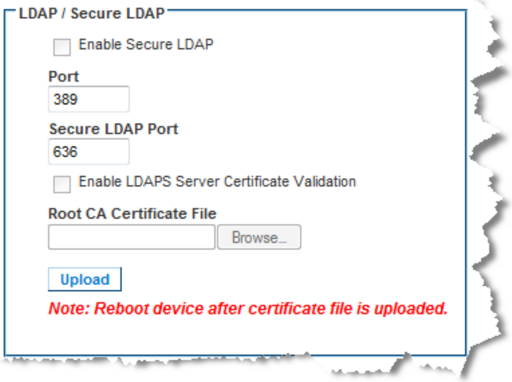


LDAP/セキュア LDAP

13. SSL を使用する場合は、[Enable Secure LDAP] (セキュア LDAP を有効にする) チェックボックスをオンにします。これにより、[Enable LDAPS Server Certificate Validation] (LDAPS サーバ証明書の検証を有効にする) チェックボックスがオンになります。Secure Sockets Layer (SSL) は、KSX II が LDAP/LDAPS サーバと安全に通信できるようにする暗号プロトコルです。
14. [Port] (ポート) のデフォルトは 389 です。標準 LDAP TCP ポートを使用するか、または別のポートを指定します。
15. [Secure LDAP Port] (セキュア LDAP ポート) のデフォルトは 636 です。デフォルトのポートを使用するか、または別のポートを指定します。このフィールドは、[Enable Secure LDAP] (セキュア LDAP を有効にする) チェックボックスがオンのときにのみ使用します。
16. 前にアップロードしたルート CA 証明書ファイルを使用してサーバから提供された証明書を検証するには、[Enable LDAPS Server Certificate Validation] (LDAPS サーバ証明書の検証を有効にする) チェックボックスをオンにします。前にアップロードしたルート CA 証明書ファイルを使用しない場合は、このチェックボックスをオフのままにします。この機能を無効にすることは、不明な証明機関によって署名された証明書を受け取ることと同じです。このチェックボックスは、[Enable Secure LDAP] (セキュア LDAP を有効にする) チェックボックスがオンのときにのみ使用できます。

注: 検証にルート CA 証明書を使用し、さらに [Enable LDAPS Server Certificate Validation] (LDAPS サーバ証明書の検証を有効にする) チェックボックスをオンにする場合は、サーバ ホスト名がサーバ証明書に記載された共通名と一致する必要があります。

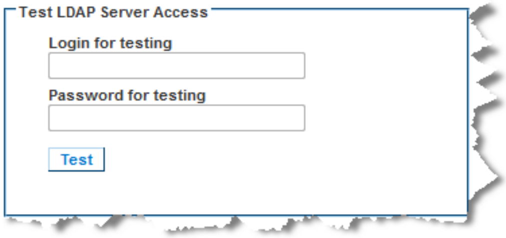
17. 必要な場合は、ルート CA 証明書のファイルをアップロードします。このフィールドは、[セキュア LDAP を有効にする] チェックボックスがオンのときに有効になります。LDAP/LDAPS サーバ用の Base64 エンコードの X-509 形式の CA 証明書ファイルについては、担当の認証サーバ管理者に問い合わせてください。[参照] を使用して証明書ファイルを選択します。LDAP/LDAPS サーバの証明書を新しい証明書に置き換える場合は、新しい証明書を有効にするために KSX II を再起動する必要があります。



LDAP サーバ アクセスのテスト

18. LDAP サーバおよび KSX II をリモート認証用に正しく構成するために複雑な設定が必要になることがあるので、KSX II には、[Authentication Settings] (認証設定) ページから LDAP の設定をテストする機能が用意されています。LDAP の設定をテストするには、[Login for testing] (テスト用ログイン) フィールドと [Password for testing] (テスト用パスワード) フィールドにそれぞれログイン名とパスワードを入力します。これは、KSX II にアクセスするときに入力したユーザ名とパスワードです。LDAP サーバはこれを使用してユーザを認証します。[Test] (テスト) をクリックします。

19. テストが完了すると、テストが成功したことを知らせるメッセージが表示されます。テストが失敗した場合は、詳細なエラー メッセージが表示されます。成功したことが表示されるか、または失敗した場合は詳細なエラー メッセージが表示されます。成功時には、リモート LDAP サーバから取得されたテスト ユーザのグループ情報も表示されることがあります。



ユーザ グループ情報を Active Directory サーバから返す

KSX II では Active Directory® (AD) を使用したユーザ認証がサポートされているので、ユーザを KSX II でローカルに定義する必要はありません。これにより、Active Directory のユーザ アカウントとパスワードは、AD サーバ上に排他的に維持されます。認可と AD ユーザ特権は、標準の KSX II ポリシー、および AD ユーザ グループにローカルに適用されるユーザ グループ特権によって制御および管理されます。

重要: Raritan, Inc. の既存のお客様がすでに AD スキーマを変更して Active Directory サーバを設定している場合、KSX II はこの設定をサポートします。この場合、以下に示す手順を実行する必要はありません。AD LDAP/LDAPS スキーマを更新する方法の詳細については、「LDAP スキーマの更新」を参照してください。

▶ KSX II で AD サーバを有効にするには、以下の手順に従います。

1. KSX II を使用して、特殊なグループを作成し、適切な許可および特権をグループに割り当てます。たとえば、KVM_Admin や KVM_Operator というグループを作成します。
2. Active Directory サーバで、前の手順で作成したのと同じグループ名を持つ新しいグループを作成します。
3. AD サーバ上で、手順 2 で作成したグループに KSX II ユーザを割り当てます。
4. KSX II で、AD サーバを有効にし、適切に設定します。「LDAP/LDAPS リモート認証の実装」を参照してください。

重要な注記:

- グループ名では大文字と小文字が区別されます。
- KSX II には、[管理者] と [<不明>] のデフォルト グループが用意されています。これらのグループを変更したり削除したりすることはできません。Active Directory サーバでこれらと同じグループ名が使用されていないことを確認してください。
- Active Directory サーバから返されたグループ情報が KSX II のグループ設定と一致しない場合、正常に認証されたユーザに対して自動的に [<不明>] グループが割り当てられます。
- ダイヤルバック番号を使用する場合は、次の文字列を入力する必要があります。大文字と小文字は区別されます。*msRADIUSCallbackNumber*
- Microsoft からの推奨に基づいて、ドメイン ローカル グループではなく、ユーザ アカウントを含むグローバル グループを使用する必要があります。

RADIUS リモート認証の実装

Remote Authentication Dial-in User Service (RADIUS) は、ネットワーク アクセス アプリケーションのための AAA (認証 (authentication)、認可 (authorization)、アカウンティング (accounting)) プロトコルです。

▶ RADIUS 認証プロトコルを使用するには、以下の手順に従います。

1. [User Management] (ユーザ管理) の [Authentication Settings] (認証設定) をクリックして、[Authentication Settings] (認証設定) をページを開きます。
2. [RADIUS] (RADIUS) ラジオ ボタンをクリックして、ページの [RADIUS] (RADIUS) セクションを有効にします。
3. RADIUS アイコンをクリックして、ページの [RADIUS] (RADIUS) セクションを展開します。
4. [Primary Radius Server] (プライマリ Radius サーバ) フィールドおよび [Secondary Radius Server] (セカンダリ Radius サーバ) フィールドに、プライマリ認証サーバの IP アドレスおよびオプションでセカンダリ認証サーバの IP アドレスを入力します (最大 256 文字)。
5. [Shared Secret] (共有の秘密) フィールドに、認証に使用するサーバの秘密フレーズを入力します (最大 128 文字)。

   共有の秘密とは、KSX II と RADIUS サーバとの間で安全に通信を行うために両者で共有される文字列です。これは、基本的にはパスワードです。
6. [Authentication Port] (認証ポート) のデフォルトは 1812 ですが、必要に応じて変更できます。
7. [Accounting Port] (アカウンティング ポート) のデフォルトは 1813 ですが、必要に応じて変更できます。

8. [Timeout]（タイムアウト）は秒単位で記録され、デフォルトは 1 秒ですが、必要に応じて変更できます。

   このタイムアウトは、KSX II が次の認証要求を送信する前に RADIUS サーバからの応答を待つ時間です。

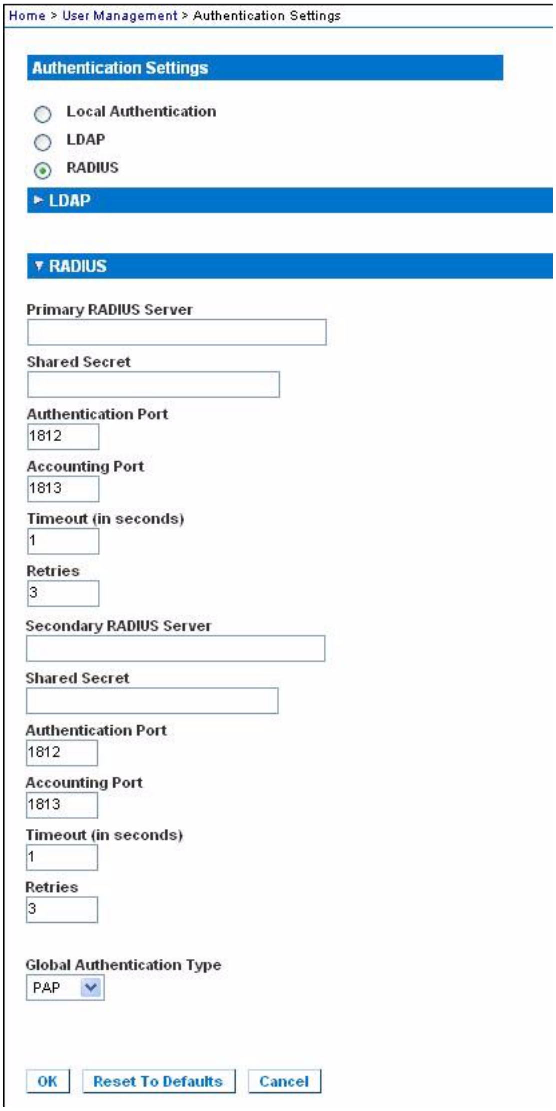
9. デフォルトの再試行回数は 3 回です。

   これは、KSX II が RADIUS サーバに対して認証要求を送信する回数です。

10. ドロップダウン リストのオプションから、適切な [Global Authentication Type]（グローバル認証タイプ）を選択します。

    - [PAP] (PAP) – PAP の場合、パスワードは平文（ひらぶん）– 暗号化されないテキストとして送信されます。PAP は対話型ではありません。サーバがログイン プロンプトを送信してその応答を待つ方式ではなく、接続が確立された時点でユーザ名とパスワードが 1 つのデータ パッケージとして送信されます。

- [CHAP] (CHAP) - CHAP の場合、サーバはいつでも認証を要求できます。CHAP は、PAP よりも高いセキュリティを実現します。



ユーザ グループ情報を RADIUS 経由で返す

RADIUS 認証の試行が成功したら、KSX II は、ユーザのグループの許可に基づいて、そのユーザの許可を決定します。

リモート RADIUS サーバは、RADIUS FILTER-ID として実装された属性を返すことによって、これらのユーザ グループ名を提供できます。FILTER-ID は、Raritan:G{*GROUP_NAME*} という形式となります。*GROUP_NAME* は、ユーザが属するグループの名前を示す文字列です。

`Raritan:G{GROUP_NAME}:D{Dial Back Number}`

GROUP_NAME は、ユーザが属するグループの名前を示す文字列です。Dial Back Number は、ユーザ アカウントに関連付けられている番号で、KSX II モデムがユーザ アカウントへのダイヤルバックに使用します。

RADIUS 通信交換仕様

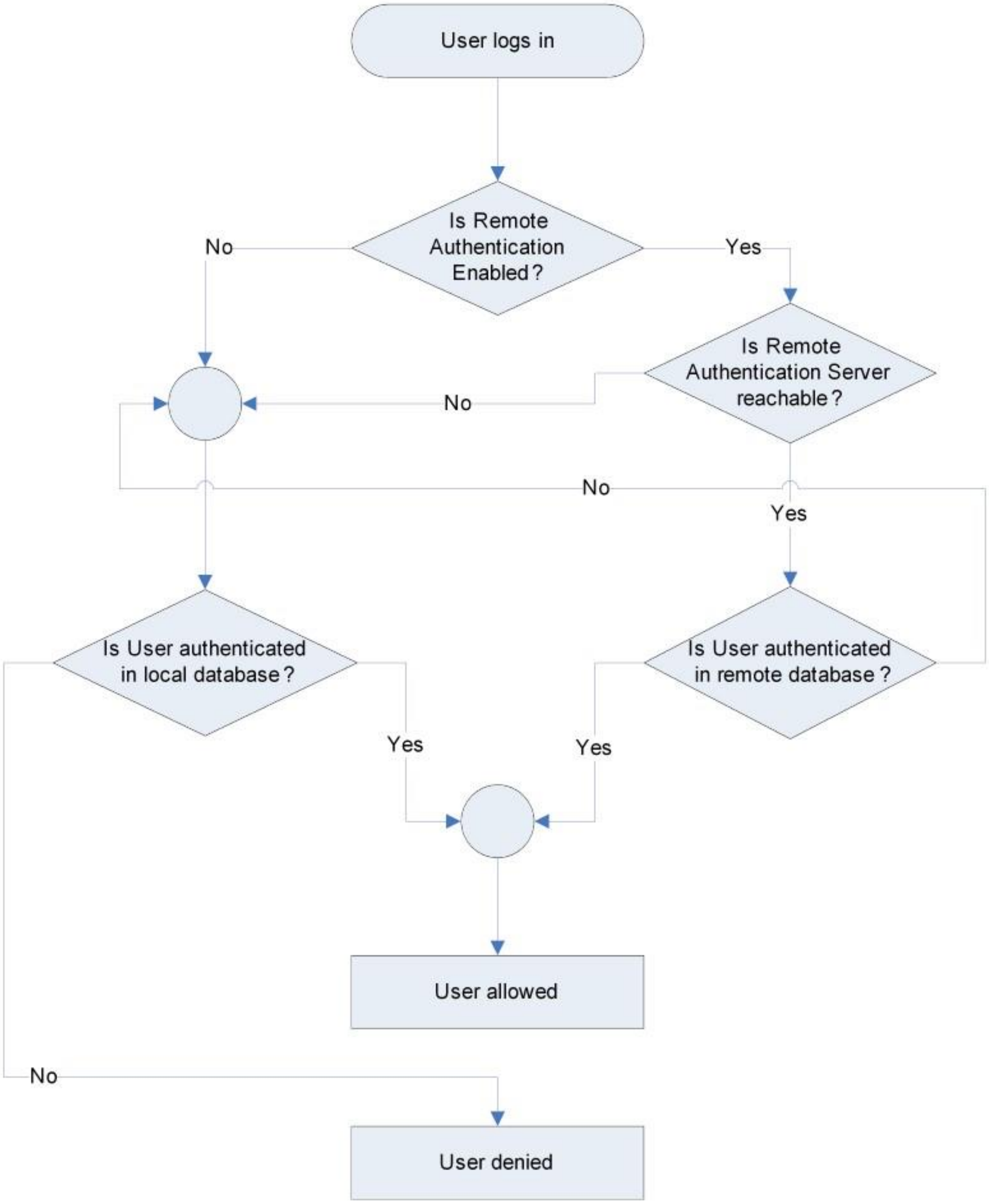
KSX II は、以下の RADIUS 属性を RADIUS サーバに送信します。

属性	データ
ログイン	
Access-Request(1)	
NAS-Port-Type (61)	ネットワーク接続の場合は VIRTUAL (5)
NAS-IP-Address (4)	KSX II の IP アドレス
User-Name (1)	ログイン画面で入力されたユーザ名
Acct-Session-ID (44)	アカウンティングのセッション ID
User-Password(2):	暗号化されたパスワード
Accounting-Request(4)	
Acct-Status (40)	Start(1) - アカウンティングを開始する
NAS-Port-Type (61)	ネットワーク接続の場合は VIRTUAL (5)
NAS-Port (5)	常に 0
NAS-IP-Address (4)	KSX II の IP アドレス
User-Name (1)	ログイン画面で入力されたユーザ名
Acct-Session-ID (44)	アカウンティングのセッション ID
ログアウト	
Accounting-Request(4)	

属性	データ
Acct-Status (40)	Stop(2) - アカウンティングを停止する
NAS-Port-Type (61)	ネットワーク接続の場合は VIRTUAL (5)
NAS-Port (5)	常に 0
NAS-IP-Address (4)	KSX II の IP アドレス
User-Name (1)	ログイン画面で入力されたユーザ名
Acct-Session-ID (44)	アカウンティングのセッション ID

ユーザ認証プロセス

リモート認証は、その後のフローチャートに指定されたプロセスに従います。

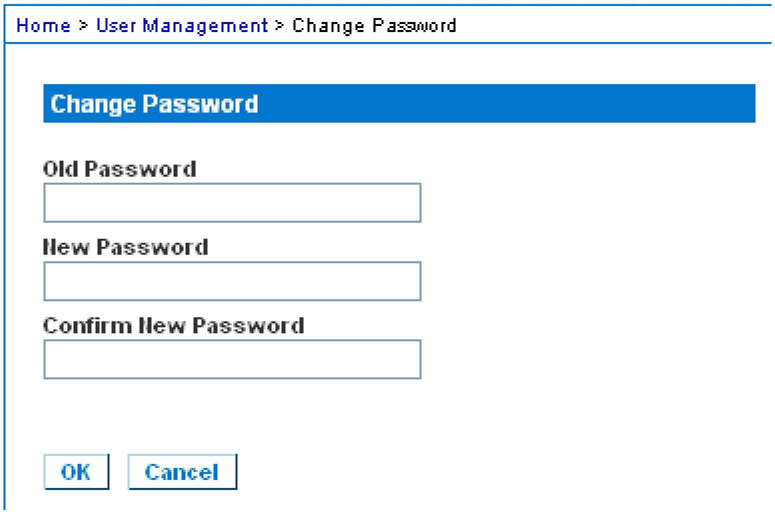


パスワードの変更

▶ **KSX II パスワードを変更するには、以下の手順に従います。**

1. [User Management] (ユーザ管理) の [Change Password] (パスワードの変更) を選択します。[Change Password] (パスワードの変更) ページが開きます。
2. [Old Password] (旧パスワード) フィールドに現在のパスワードを入力します。
3. [New Password] (新しいパスワード) フィールドに新しいパスワードを入力します。[Confirm New Password] (新しいパスワードの確認) フィールドにパスワードを再入力します。パスワードには、最大 64 文字の英数字と特殊文字を使用できます。
4. [OK] をクリックします。
5. パスワードが正常に変更された旨のメッセージが表示されます。[OK] をクリックします。

*注:強力なパスワードが使用されている場合は、パスワードに必要な形式に関する情報がこのページに表示されます。パスワードと強力なパスワードについての詳細は、オンライン ヘルプの「*Strong Passwords (強力なパスワード) 『210*p.* の「[Strong Passwords] (強力なパスワード)*"参照 』」を参照してください。*



Ch 8 デバイス管理

この章の内容

ネットワーク設定 147
[Device Services] (デバイス サービス) 153
モデムを設定する 160
日付/時刻の設定 162
イベント管理 162
ポートの設定 169
ポート キーワード 204
ポート グループ管理 206

ネットワーク設定

[Network Settings] (ネットワーク設定) ページを使用して、KSX II のネットワーク設定 (たとえば、IP アドレス、検出ポート、LAN インタフェース パラメータなど) をカスタマイズします。

IP 設定を行うには 2 つのオプションがあります。

- [None] (なし) (デフォルト) – 推奨されるオプションです (静的 IP)。KSX II はネットワーク インフラストラクチャの一部であるため、IP アドレスを頻繁に変更されると手間がかかります。このオプションにより、ネットワーク パラメータを固定できます。
- [DHCP] (DHCP) – DHCP サーバによって IP アドレスが自動的に割り当てられます。

▶ ネットワーク設定を変更するには、以下の手順に従います。

1. [Device Settings] (デバイス設定) の [Network] (ネットワーク) を選択します。[ネットワーク設定] (Network Settings) ページが開きます。
2. ネットワーク基本設定を更新します。「*ネットワーク基本設定*『*148*p. 』」を参照してください。
3. LAN インタフェースの設定を更新します。「*LAN インタフェース設定* 『*152*p. 』」を参照してください。
4. [OK] (OK) をクリックして、これらの設定を保存します。変更を適用するために再起動が必要な場合は、再起動メッセージが表示されます。

▶ 工場出荷時のデフォルトに戻すには、以下の手順に従います。

- [Reset to Defaults] (デフォルトに戻す) をクリックします。

ネットワーク基本設定

ここでは、[Network Settings] (ネットワーク設定) ページで IP アドレスを割り当てる方法について説明します。このページのすべてのフィールドおよび操作についての詳細は、「*ネットワーク設定* 『*147*p. 』」を参照してください。

▶ IP アドレスを割り当てるには、次の手順に従います。

1. [Device Settings] (デバイス設定) の [Network] (ネットワーク) を選択します。[ネットワーク設定] (Network Settings) ページが開きます。
2. KSX II デバイスにわかりやすいデバイス名を指定します。最大 32 文字の英数字と有効な特殊文字を組み合わせて使用できます。スペースは使用できません。
3. [IPv4] (IPv4) セクションで、IPv4 固有の適切なネットワーク設定を入力するか、選択します。
   a. 必要に応じて IP アドレスを入力します。デフォルトの IP アドレスは「192.168.0.192」です。
   b. サブネット マスクを入力します。デフォルトのサブネット マスクは「255.255.255.0」です。
   c. [IP Auto Configuration] (IP 自動設定) ドロップダウンから [None] (なし) を選択した場合は、デフォルトのゲートウェイを入力します。
   d. [IP Auto Configuration] (IP 自動設定) ドロップダウンから [DHCP] (DHCP) を選択した場合は、優先ホスト名を入力します。
   e. [IP Auto Configuration] (IP 自動設定) を選択します。次のオプションを使用できます。
   - [None] (なし) (静的 IP) – このオプションを選択した場合は、ネットワーク パラメータを手動で指定する必要があります。

     KSX II はインフラストラクチャ デバイスであり、IP アドレスは変更されないので、このオプションが推奨されます。
   - [DHCP] (DHCP) – DHCP サーバから一意の IP アドレスとその他のパラメータを取得するために、ネットワークに接続しているコンピュータ (クライアント) によって Dynamic Host Configuration Protocol が使用されます。

     このオプションを選択した場合、ネットワーク パラメータは DHCP サーバによって割り当てられます。DHCP を使用する場合は、[Preferred host name] (優先ホスト名) を入力します (DHCP のみ)。最大 63 文字まで使用できます。
4. IPv6 を使用する場合は、[IPv6] セクションで、適切な IPv6 固有のネットワーク設定を入力するか、選択します。
   a. セクション内のフィールドを有効にするには、[IPv6] チェックボックスをオンにします。

b. [Global/Unique IP Address] (グローバル/一意の IP アドレス) を入力します。これは、KSX II に割り当てられる IP アドレスです。

c. [Prefix Length] (固定長) を入力します。これは、IPv6 アドレスで使用されるビット数です。

d. [Gateway IP Address] (ゲートウェイ IP アドレス) を入力します。

e. [Link-Local IP Address] (リンク - ローカル IP アドレス)。このアドレスは、自動的にデバイスに割り当てられます。これは、近隣探索、またはルータが存在しない場合に使用されます。**[Read-Only] (読み取り専用)**

f. [Zone ID]。これは、アドレスが関連付けられているデバイスを識別します。**[Read-Only] (読み取り専用)**

g. [IP Auto Configuration] (IP 自動設定) を選択します。次のオプションを使用できます。

- [None] (設定しない) - 自動 IP 設定を使用せず、IP アドレスを自分で設定する場合は、このオプションを選択します (静的 IP)。推奨されるデフォルトのオプションです。

  [IP auto configuration] (IP 自動設定) で [None] (設定しない) を選択すると、[Network Basic Settings] (ネットワーク基本設定) フィールド ([Global/Unique IP Address] (グローバル/一意の IP アドレス)、[Prefix Length] (固定長)、[Gateway IP Address] (ゲートウェイ IP アドレス)) が有効になり、IP アドレスを手動で設定できるようになります。

- [Router Discovery] (ルータ検出) - このオプションを使えば、グローバルな IPv6 アドレスまたは、ローカルにリンクしたアドレスを大きく超えるユニーク ローカルの IPv6 に自動的に割り当てられます。これはサブネットへの直接接続に限定して適用されます。

5. [DHCP] が選択され、[Obtain DNS Server Address] (DNS サーバ アドレスを取得) が有効になっている場合は、[Obtain DNS Server Address Automatically] (DNS サーバ アドレスを自動的に取得) を選択します。[Obtain DNS Server Address Automatically] (DNS サーバ アドレスを自動的に取得) が選択されると、DHCP サーバが提供する DNS 情報が使用されます。

6. [Use the Following DNS Server Addresses] (次の DNS サーバ アドレスを使用) を選択する場合は、[DHCP] が選択されているかどうかにかかわらず、このセクションに入力されたアドレスが、DNS サーバの接続に使用されます。

   [Use the Following DNS Server Addresses] (次の DNS サーバ アドレスを使用) オプションを選択する場合は、次の情報を入力します。これらのアドレスは、停電によりプライマリ DNS サーバ接続が切断された場合に使用されるプライマリおよびセカンダリ DNS アドレスです。

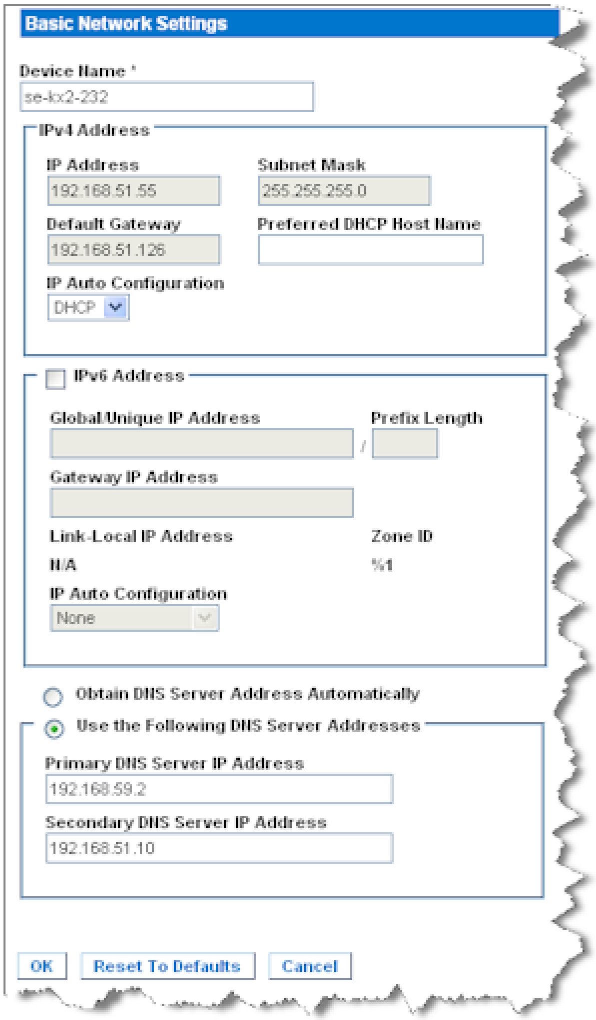
a. [Primary DNS Server IP Address] (プライマリ DNS サーバ IP アドレス)
b. [Secondary DNS Server IP Address] (セカンダリ DNS サーバ IP アドレス)

7. 完了したら [OK] をクリックします。

[Network Settings] (ネットワーク設定) ページのこのセクションの設定についての詳細は、「*LAN インタフェース設定* 『*152*p. 』」を参照してください。

---

*注: 一部の環境では、[LAN Interface Speed & Duplex] (LAN インタフェースの速度と二重化) のデフォルトである [Autodetect] (自動検出) (自動ネゴシエーション) が選択されている場合にネットワーク パラメータが適切に設定されず、ネットワーク上の問題が発生する場合があります。そのような場合は、KSX II の [LAN Interface Speed & Duplex] (LAN インタフェースの速度と二重化) フィールドを [100 Mbps/Full Duplex] (またはネットワークに合ったオプション) に設定することで問題を解決できます。詳細は、「*ネットワーク設定 『147*p. 』」を参照してください。*



LAN インタフェース設定

現在のパラメータ設定は、[Current LAN interface parameters] (現在の LAN インタフェース パラメータ) フィールドで確認します。

1. [Device Settings] (デバイス設定) の [Network] (ネットワーク) を選択します。[ネットワーク設定] (Network Settings) ページが開きます。
2. 以下の [LAN Interface Speed & Duplex] (LAN インタフェースの速度と二重化) のオプションから適切なものを選択します。
   - [Autodetect] (自動検出) (デフォルト オプション)
   - [10 Mbps/Half] (10 Mbps/半二重) – 両方の LED が点滅
   - [10 Mbps/Full] (10 Mbps/全二重) – 両方の LED が点滅
   - [100 Mbps/Half] (100 Mbps/半二重) – 黄色の LED が点滅
   - [100 Mbps/Full] (100 Mbps/半二重) – 黄色の LED が点滅
   - [1000 Mbps/Full] (1000 Mbps/全二重) (ギガビット) – 緑色の LED が点滅
   - [Half-duplex] (半二重) の場合、双方向の通信は可能ですが、一度に通信できるのは一方向だけです (同時に通信できません)。
   - [Full-duplex] (全二重) の場合、同時に双方向の通信が可能です。

   注:半二重または全二重で 10 Mbps で実行しているときに、問題が発生する場合があります。問題が発生した場合は、別の速度と二重化の設定を選択してください。

   詳細は、「*Network Speed Settings* 『*318*p. の"*ネットワーク速度の設定*"参照 』」を参照してください。
3. この [Enable Automatic Failover] (自動フェイルオーバを有効にする) チェックボックスをオンにすると、アクティブなネットワーク ポートに障害が発生した場合、KSX II では 2 番目のネットワーク ポートを使用して、自動的にネットワーク接続を回復します。

   注: フェイルオーバ ポートは実際にフェイルオーバが発生するまで有効にならないので、ポートを監視しないか、フェイルオーバが発生した後にのみ監視するようにすることをお勧めします。

   このオプションを有効にすると、次の 2 つのフィールドが使用されます。
   - [Ping Interval (seconds)] (Ping インターバル (秒)) – Ping インターバルの設定により、KSX II が指定されたゲートウェイへのネットワーク パスの状態をチェックする頻度が決まります。デフォルトの Ping インターバルは 30 秒です。
   - [Timeout (seconds)] (タイムアウト (秒)) – タイムアウトの設定により、指定されたゲートウェイにネットワーク接続経由でアクセスできなくなってからフェイルオーバが発生するまでの時間が決まります。

注: Ping インターバルとタイムアウトは、ローカル ネットワーク状態に合わせて最適な値に設定できます。タイムアウトは、送信する 2 つ以上の Ping 要求と返される応答に対応できるように設定する必要があります。たとえば、ネットワークの利用率が高いためにフェイルオーバの発生する確率が高い場合は、タイムアウトを Ping インターバルの 3 ～ 4 倍に延ばす必要があります。

4. 帯域幅を選択します。
5. [OK] をクリックして LAN 設定を適用します。

[Device Services] (デバイス サービス)

[Device Services] (デバイス サービス) ページでは、次のことができます。

- Telnet 接続を有効にする
- SSH アクセスを有効にする
- HTTP ポートおよび HTTPS ポートの設定を指定する
- シリアル コンソール アクセスを有効にする
- 検出ポート アクセスを設定する
- ダイレクト ポート アクセスを有効にする
- AKC を使用している場合に、AKC ダウンロード サーバ証明書の検証を有効にする

Telnet 接続を有効にする

Telnet を使用して KSX II に接続したい場合、まず、CLI またはブラウザを使用して KSX II に接続します。

▶ Telnet 接続を有効にするには

1. [Device Settings] (デバイス設定) を選択し、[Enable TELNET Access] (TELNET アクセスを有効にする) チェックボックスを選択します。
2. Telnet ポートを入力します。
3. [OK] をクリックします。

Telnet 接続が有効になったら、Telnet を使用して KSX II に接続し、他のパラメータ値を設定することができます。

SSH を有効にする

管理者が SSH v2 アプリケーションを使用して KSX II にアクセスできるようにするには、[Enable SSH Access] (SSH アクセスを有効にする) チェック ボックスをオンにします。

▶ SSH アクセスを有効にするには

1. [Device Settings(デバイス設定)] > [Device Services(デバイス サービス)] をクリックします。[Device Services(デバイス サービス)] ページが開きます。
2. [Enable SSH Access] (SSH アクセスを有効にする) を選択します。
3. [SSH Port Information] (SSH ポート情報) を入力します。標準の SSH TCP ポート番号は 22 ですが、ポート番号を変更して高いレベルのセキュリティ処理を提供することもできます。
4. [OK] (OK) をクリックします。

HTTP ポートおよび HTTPS ポートの設定

KSX II によって使用される HTTP ポートまたは HTTPS ポートを設定できるようになりました。 たとえば、デフォルトの HTTP ポートであるポート 80 を別の用途で使用している場合、HTTP 用ポートを変更すると、ポート 80 が HTTP 用として使用されなくなります。

▶ HTTP ポートまたは HTTPS ポートの設定を変更するには

1. [Device Settings(デバイス設定)] > [Device Services(デバイス サービス)] をクリックします。[Device Services(デバイス サービス)] ページが開きます。
2. [HTTP Port] (HTTP ポート) フィールドまたは [HTTPS Port] (HTTPS ポート) フィールド (あるいはその両方) に新しいポート番号を入力します。
3. [OK] (OK) をクリックします。

検出ポートを入力する

KSX II の検出は、設定可能な 1 つの TCP ポートで行われます。デフォルトではポート 5000 に設定されていますが、80 と 443 以外であれば、どの TCP ポートを使用するよう設定してもかまいません。ファイアウォールの外側から KSX II にアクセスするには、お使いのファイアウォールの設定で、デフォルト ポート 5000 または上記で設定したデフォルト以外のポートを使用する双方向通信を有効にする必要があります。

▶ 検出ポートを有効にするには

1. [Device Settings(デバイス設定)] > [Device Services(デバイス サービス)] をクリックします。[Device Services(デバイス サービス)] ページが開きます。
2. [Discovery Port] (検出ポート) を入力します。
3. [OK] (OK) をクリックします。

シリアル コンソール アクセスを有効にする

▶ シリアル コンソール アクセスを有効にするには、以下の手順に従います。

1. [Device Settings(デバイス設定)] > [Device Services(デバイス サービス)] をクリックします。[Device Services(デバイス サービス)] ページが開きます。
2. [Enable Serial Console Access] (シリアル コンソール アクセスを有効にする) を選択します。
3. デバイスのボー レートを選択します。
4. [OK] をクリックします。

URL を経由したダイレクト ポート アクセスの有効化

ダイレクト ポート アクセス機能を利用した場合、ユーザはデバイスの [Login] (ログイン) ダイアログ ボックスと [Port Access] (ポート アクセス) ページを使用する必要がなくなります。

この機能を使用すると、ユーザ名とパスワードが URL に含まれていない場合に、ユーザ名とパスワードを直接入力してターゲットにアクセスすることもできます。

ダイレクト ポート アクセスに関する重要な URL 情報は次のとおりです。

VKC とダイレクト ポート アクセスを使用する場合:

- https://IPaddress/dpa.asp?username=username&password=password&port=port number

AKC とダイレクト ポート アクセスを使用する場合:

- https://IPaddress/dpa.asp?username=username&password=password&port=port number&client=akc

説明:

- username と password はオプションです。指定しない場合はログイン ダイアログ ボックスが表示され、認証後、ユーザはターゲットに直接接続されます。
- port には、ポート番号またはポート名を指定できます。ポート名を使用する場合は、一意の名前にしなければ、エラーが報告されます。port を省略した場合もエラーが報告されます。
- ブレード シャーシの場合、port は「<port number>'-'<slot number>」の形式で指定します。たとえば、ポート 1、スロット 2 に接続されたブレード シャーシの場合は「1-2」のように指定します。
- client=akc は、AKC クライアントを使用しない場合はオプションです。client=akc を指定しない場合、VKC がクライアントとして使用されます。

▶ ダイレクト ポート アクセスを有効するには、以下の手順に従います。

1. [Device Settings(デバイス設定)] > [Device Services(デバイス サービス)] をクリックします。[Device Services(デバイス サービス)] ページが開きます。
2. URL で必要なパラメータを渡してユーザに Dominion デバイス経由でターゲットに直接アクセスさせる場合は、[Enable Direct Port Access via URL] (URL を介したダイレクト ポート アクセスを有効にする) を選択します。
3. [OK] をクリックします。

Telnet、IP アドレス、または SSH 経由のダイレクト ポート アクセスの構成

このトピックの情報は、シリアル ターゲット向けにダイレクト ポート アクセスを有効にする方法を取り上げたものです。KSX II への KVM/シリアル ポート接続用にダイレクト ポート アクセスを有効にするには、[Device Services] (デバイス サービス) ページで [Enable Direct Port Access via URL] (URL を介したダイレクト ポート アクセスを有効にする) チェックボックスをオンにします。「*URL を経由したダイレクト ポート アクセスの有効化* 『*156*p. 』」を参照してください。

▶ ダイレクト ポート アクセスを設定するには、以下の手順に従います。

1. [Device Settings] (デバイス設定) の [Device Services] (デバイス サービス) を選択します。[Device Service Settings] (デバイス サービス設定) ページが開きます。
2. SSH および Telnet に使用する IP アドレスとポートをシリアル ターゲットの該当するフィールドに入力します。

   3 つすべてのフィールドを空白のままにしておくと、シリアル ターゲットのダイレクト ポート アクセスが無効になります。ダイレクト ポート アクセスを有効にするには、以下のいずれかを実行する必要があります。

   - グローバル Telnet または SSH アクセスを有効にします。
   - 3 つのフィールドのうち少なくとも 1 つのフィールドに、有効な IP アドレスまたは TCP ポートを入力します。

   重要: 複数のフィールドに入力することは推奨されません。

   以下は、Telnet と IP の例です。

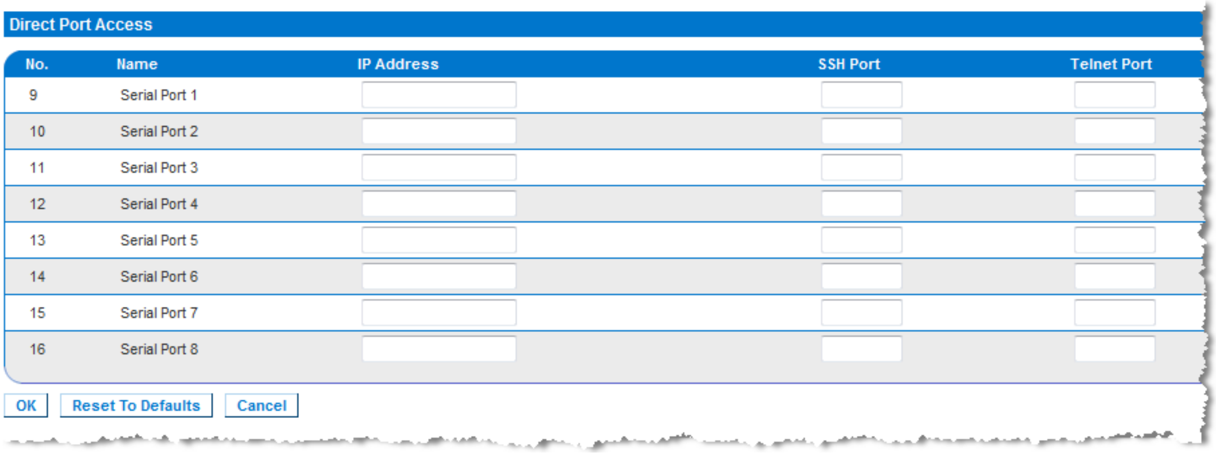
   - IP エイリアス アドレス経由のダイレクト ポート アクセス:

     シリアル ターゲットの IP エイリアス アドレス 192.168.1.59 を設定します。これが完了したら、"telnet 192.168.1.59" を使用して、Telnet 経由でターゲットにアクセスできます。
   - Telnet ポート経由のダイレクト ポート アクセス:

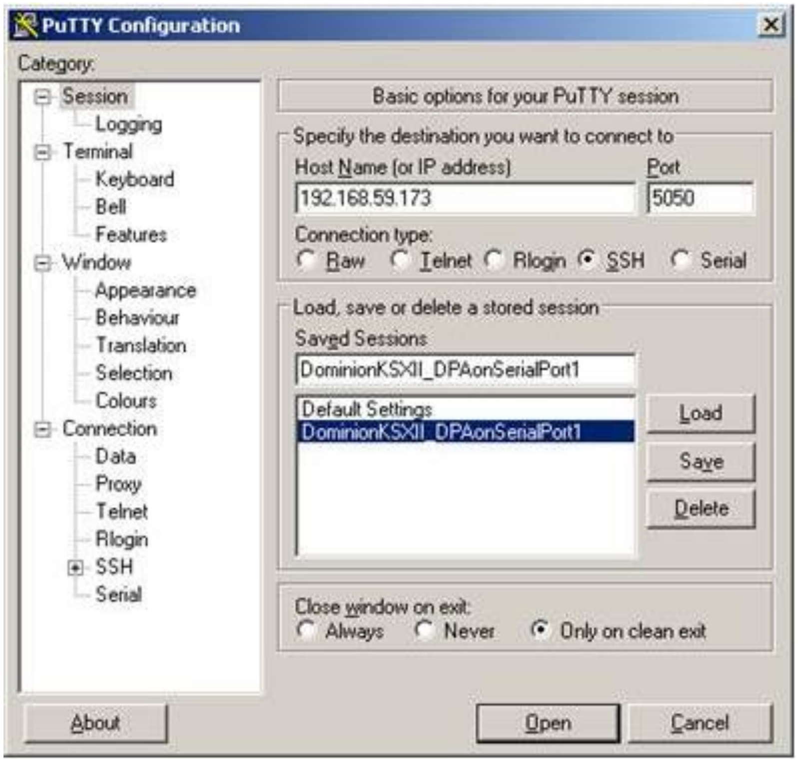
     Telnet TCP ポートを "7770" に設定します。これが完了したら、"telnet <KSX II device IP address> 7770" を使用して、ターゲットにアクセスできます。
   - SSH ポート経由のダイレクト ポート アクセス:

     SSH TCP ポートを "7888" に設定します。これが完了したら、"ssh -l <login> <KSX II device IP address> –p 7888" を使用して、ターゲットにアクセスできます。

3. [OK] をクリックしてこの情報を保存します。



ダイレクト ポート アクセスを作成したら、PuTTY などのクライアント アプリケーションで接続することができます。次に、ダイレクト ポート アクセス情報が PuTTY に表示される例を示します。クライアント アプリケーションとして使用できるのは、PuTTY だけではありません。ここでは、例示するためにのみ PuTTY を使用しています。



AKC ダウンロード サーバ証明書の検証の有効化

AKC クライアントを使用する場合は、[Enable AKC Download Server Certificate Validation (AKC ダウンロード サーバ証明書の検証を有効にする)] 機能を使用するかどうかを選択できます。

注:[Enable AKC Download Server Certificate Validation] (AKC ダウンロード サーバ証明書の検証を有効にする) 機能と共に IPv4 および IPv6 デュアル スタック モードで動作している場合、Microsoft® ClickOnce® では、サーバ証明書 CN に IPv6 アドレスのゼロ圧縮形式を含めてはなりません。

ゼロ圧縮形式を含めると、AKC を正常にダウンロードして起動することができなくなります。

ただし、これは IPv6 アドレスの形式に対するブラウザの設定と競合する場合があります。

共通名 (CN) でサーバのホスト名を使用するか、証明書の「サブジェクトの別名」に IPv6 アドレスの圧縮形式や非圧縮形式を含めてください。

オプション 1: AKC ダウンロード サーバ証明書の検証を有効にしない (デフォルト設定)

AKC ダウンロード サーバ証明書の検証を有効にしない場合は、以下の操作を行います。すべての Dominion デバイス ユーザおよび CC-SG Bookmark and Access Client ユーザは、次のことを行う必要があります。

- アクセスするデバイスの IP アドレスからの Cookie が現在ブロックされていないことを確認します。
- Windows Vista、Windows 7、および Windows 2008 Server のユーザは、アクセスするデバイスの IP アドレスがブラウザの [信頼済みサイト] ゾーンに含まれ、デバイスへのアクセス時に保護モードが有効になっていないことを確認する必要があります。

オプション 2: AKC ダウンロード サーバ証明書の検証を有効にする

AKC ダウンロード サーバ証明書の検証を有効にする場合は、以下の操作を行います。

- 管理者は、有効な証明書をデバイスにアップロードするか、自己署名証明書をデバイスで生成する必要があります。証明書で有効なホストが指定されている必要があります。
- 各ユーザは、CA 証明書 (または自己署名証明書のコピー) をブラウザの信頼されたルート証明機関ストアに追加する必要があります。
- CC-SG ネイバーフッドを使用する場合は、各ネイバーフッド メンバーの AKC を有効にする必要があります。

► **Windows Vista® または Windows 7® オペレーティング システムを使用している場合、自己署名証明書をインストールするには、以下の手順に従います。**

1. [信頼済みサイト] ゾーンに KSX II の IP アドレスを追加し、保護モードがオフになっていることを確認します。
2. URL に KSX II の IP アドレスを使用して Internet Explorer® を起動します。証明書エラー メッセージが表示されます。
3. [証明書の表示] を選択します。
4. [全般] タブで、[証明書のインストール] をクリックします。証明書が信頼されたルート証明機関ストアにインストールされます。
5. 証明書のインストール後、KSX II の IP アドレスを [Trusted Site (信頼済みサイト)] ゾーンから削除する必要があります。

► **AKC ダウンロード サーバ証明書の検証を有効にするには、以下の手順に従います。**

1. [Device Settings(デバイス設定)] > [Device Services(デバイス サービス)] をクリックします。[Device Services(デバイス サービス)] ページが開きます。
2. [Enable AKC Download Server Certificate Validation (AKC ダウンロード サーバ証明書の検証を有効にする)] チェックボックスをオンにするか、この機能を無効 (デフォルト) のままにしておくことができます。
3. [OK] をクリックします。

If you are connecting to a KSX II standalone device and support for AKC download server certificate validation is enabled, the valid IPv6 format to generate the certificate is either:

- `CN =[fd07:02fa:6cff:2500:020d:5dff:fe00:01c0]` when there is a leading 0

  or

- `CN =[fd07:02fa:6cff:2500:020d:5dff:0000:01c0]` when there is no zero compression

モデムを設定する

► **モデムを設定するには、以下の手順に従います。**

1. [Device Settings] (デバイス設定) の [Modem Settings] (モデム設定) をクリックし、[Modem Settings] (モデム設定) ページを開きます。
2. 必要な場合は、[Enable Modem] (モデムを有効にする) をオンにします。
3. [PPP server IP address] (PPP サーバ IP アドレス) にアドレスを入力します。ダイヤルアップ経由で接続を確立した場合に、KSX II に割り当てられるインターネット アドレスです。必ず入力してください。

4. [PPP Client IP address] (PPP クライアント IP アドレス) にアドレスを入力します。ダイヤルアップ経由で接続が確立された場合に、KSX II がクライアントを除外するために割り当てるインターネット アドレスです。**必ず入力してください。**

注: [PPP server IP address] (PPP サーバ IP アドレス) と [PPP Client IP address] (PPP クライアント IP アドレス) は同じ値にしないでください。 また、サーバやクライアントが使用するネットワーク アドレスとも競合しないようにしてください。

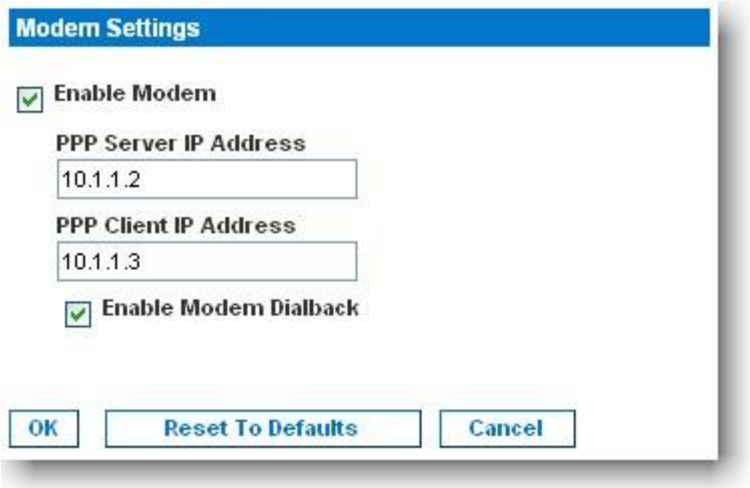
---

5. 必要な場合は、[Enable Modem Dialback] (モデムのダイヤルバックを有効にする) をオンにします。

注: ダイヤルバックを有効にした場合、モデムを介して KSX II にアクセスするユーザには、そのプロファイルでコールバック番号が定義されている必要があります。コールバック番号が定義されていない場合、ダイヤルアップはそのユーザのコールを拒否します。

---

6. [OK] をクリックして変更を確認するか、[Reset to Defaults] (デフォルトに戻す) をクリックして設定をデフォルトに戻します。



日付/時刻の設定

[Date/Time Settings] (日付/時刻の設定) ページを使用して、KSX II の日付と時刻を指定します。これには 2 とおりの方法があります。

- 手動で日付と時刻を設定する。
- 日付と時刻をネットワーク タイム プロトコル (NTP) サーバと同期する。

▶ 日付と時刻を設定するには、以下の手順に従います。

1. [Device Settings] (デバイス設定) の [Date/Time] (日付/時刻) を選択します。[Date/Time Settings] (日付/時刻の設定) ページが開きます。
2. [Time Zone] (タイム ゾーン) ドロップダウン リストから適切なタイム ゾーンを選択します。
3. 夏時間用の調整を行うには、[Adjust for daylight savings time] (夏時間用の調整) チェックボックスをオンにします。
4. 日付と時刻の設定に用いる方法を選択します。
   - [User Specified Time] (ユーザによる時刻定義) - 日付と時刻を手動で入力する場合に、このオプションを使用します。[User Specified Time] (ユーザによる時刻定義) オプションを選択した場合は、日付と時刻を入力します。時刻は、hh:mm の形式を使用します (24 時間制で入力します)。
   - [Synchronize with NTP Server] (NTP サーバと同期) - 日付と時刻をネットワーク タイム プロトコル (NTP) サーバと同期する場合に、このオプションを使用します。
5. [Synchronize with NTP Server] (NTP サーバと同期) オプションを選択した場合は、以下の手順に従います。
   a. [Primary Time server] (プライマリ タイム サーバ) の IP アドレスを入力します。
   b. [Secondary Time server] (セカンダリ タイム サーバ) の IP アドレスを入力します。Optional
6. [OK] をクリックします。

イベント管理

KSX II イベント管理機能によって、SNMP マネージャ、Syslog、監査ログへのシステム イベントの送信を有効または無効にできます。 これらのイベントはカテゴリ分けされるため、イベントごとに 1 つまたは複数の宛先に送信するかどうかを指定できます。

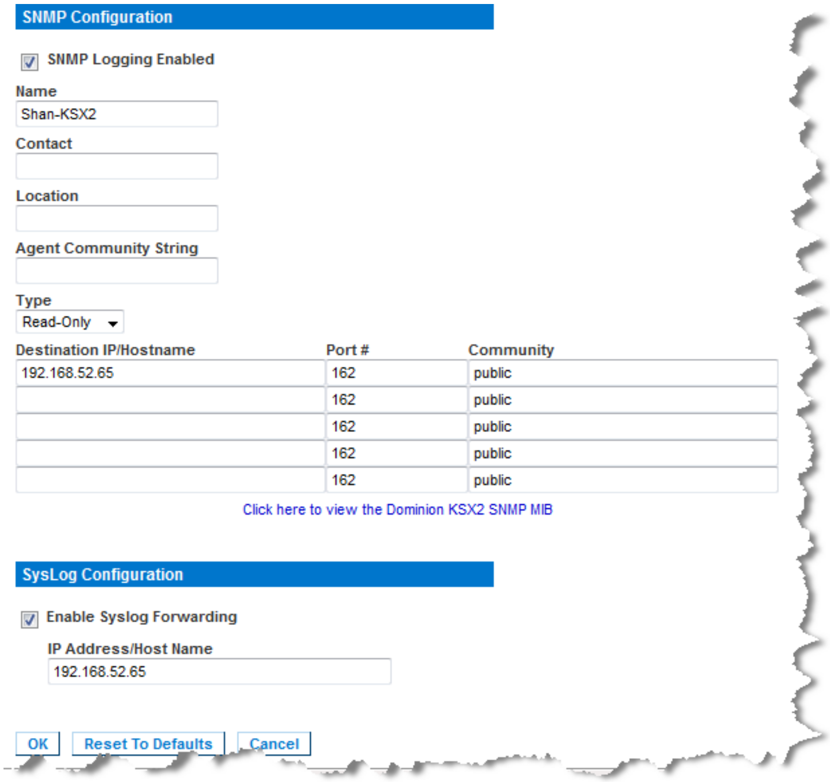
[Event Management Settings] (イベント管理設定) の設定

SNMP の設定

Simple Network Management Protocol (SNMP) は、ネットワーク管理を制御し、ネットワーク デバイスとその機能を監視するためのプロトコルです。KSX II では、イベント管理を通じて SNMP エージェントがサポートされます。

▶ **SNMP を設定する (SNMP のログ作成を有効にする) には、以下の手順に従います。**

1. [Device Settings] (デバイス設定) の [Event Management - Settings] (イベント管理 - 設定) を選択します。[Event Management - Settings] (イベント管理 - 設定) ページが開きます。



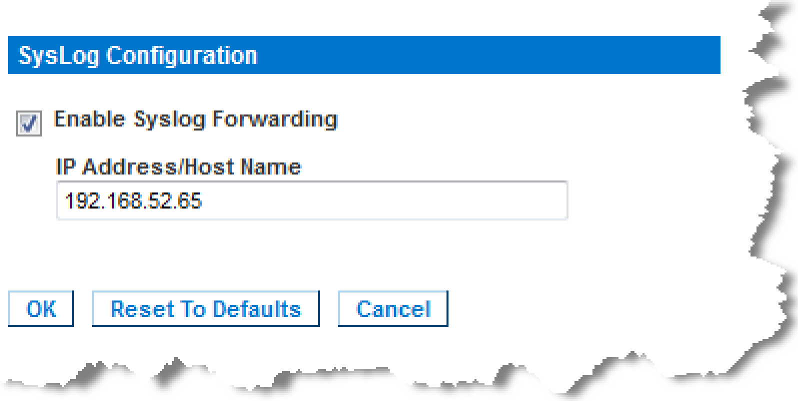
2. [Enable SNMP Logging] (SNMP ログを有効にする) オプションを選択します。これによって残りの SNMP フィールドが有効になります。
3. [Name] (名前) フィールドには、KSX II コンソール インタフェースに表示されているとおりに、SNMP エージェントの名前 (使用しているデバイスの名前) を、[Contact] (連絡先) フィールドには、そのデバイスに関連する連絡先の名前を、[Location] (所在地) フィールドには、Dominion デバイスが物理的に設置されている場所を入力します。

4. [Agent Community String] (エージェント コミュニティの文字列) (デバイスの文字列) を入力します。SNMP コミュニティとは、SNMP を実行しているデバイスと管理ステーションが所属するグループのことです。情報の送信先を定義するのに役立ちます。コミュニティ名はグループを特定するために使用されます。SNMP デバイスまたはエージェントは複数の SNMP コミュニティに所属している場合があります。
5. [Type] (タイプ) ドロップダウン リストを使用して、コミュニティに読み取り専用と読み書き可能のいずれかを指定します。
6. [Destination IP] (送信先 IP)、[Port #] (ポート番号)、[Community] (コミュニティ) を指定して、最大で 5 つの SNMP マネージャを設定します。
7. [Click here to view the Dominion SNMP MIB] (Dominion SNMP MIB を表示するにはここをクリックします) というリンクをクリックして、SNMP Management Information Base にアクセスします。
8. [OK] をクリックします。

Syslog の設定

▶ **Syslog を設定する (Syslog の送信を有効にする) には、以下の手順に従います。**

1. [Enable Syslog Forwarding] (Syslog 送信有効) オプションを選択して、リモート Syslog サーバにデバイス メッセージのログを送信します。
2. [IP Address] (IP アドレス) フィールドに Syslog サーバの IP アドレスを入力します。
3. [OK] をクリックします。



▶ 工場出荷時のデフォルトに戻すには、以下の手順に従います。

- [Reset To Defaults] (デフォルトに戻す) ボタンをクリックします。

注: IPv4 と IPv6 の両方のアドレスがサポートされています。

注: IPv6 アドレスでは、ホスト名が最大 80 文字です。

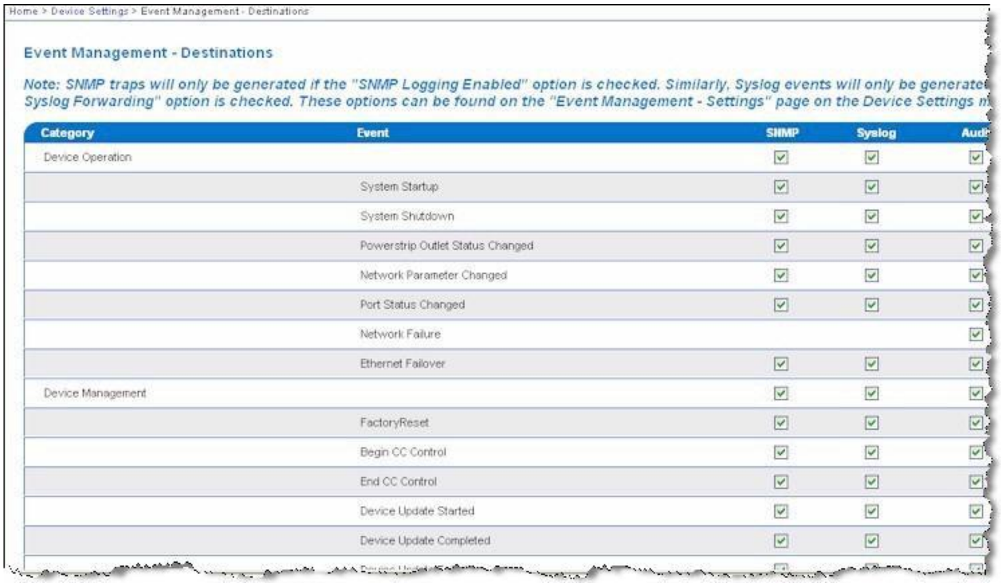
[Event Management - Destinations] (イベント管理 - 送信先) の設定

システム イベントを有効にすると、SNMP 通知イベント (トラップ) を生成できます。また、システム イベントを Syslog または監査ログにログ記録できます。[Event Management - Destinations] (イベント管理 - 送信先) ページを使用して、追跡するイベントと、その情報の送信先を選択します。

注: SNMP トラップは、[SNMP Logging Enabled] (SNMP ログを有効にする) オプションが選択されている場合にのみ生成されます。一方、Syslog イベントは、[Enable Syslog Forwarding] (Syslog 送信有効) オプションが選択されている場合にのみ生成されます。これらのオプションは、いずれも [Event Management - Settings] (イベント管理 - 設定) ページで設定します。「[Event Management - Settings] (イベント管理 - 設定)『163p. の「[Event Management Settings] (イベント管理設定) の設定"参照先 』」を参照してください。

▶ イベントとその送信先を選択するには、以下の手順に従います。

1. [Device Settings] (デバイス設定) の [Event Management - Destinations] (イベント管理 - 送信先) を選択します。[Event Management - Destinations] (イベント管理 - 送信先) ページが開きます。



システム イベントは、デバイス操作、デバイス管理、セキュリティ、ユーザ アクティビティ、ユーザ グループ管理に分類されます。

2. 有効または無効にする [Event] (イベント) ラインのアイテムと、情報の送信先のチェックボックスをオンにします。

ヒント: [Category] (カテゴリ) ラインのチェックボックスをそれぞれオンまたはオフにすると、カテゴリ全体を有効または無効に設定できます。

---

3. [OK] をクリックします。

▶ **工場出荷時のデフォルトに戻すには、以下の手順に従います。**

- [Reset To Defaults] (デフォルトに戻す) ボタンをクリックします。

SNMP トラップ設定

SNMP によって、トラップまたは通知を送信する機能と、1 つ以上の条件が満たされた場合に管理者に忠告する機能が提供されます。KSX II のトラップを次の表に示します。

トラップ名	説明
cimConnected	CIM が KSX II ポートに接続されています。
cimDisconnected	CIM が KSX II ポートから外れているか、CIM の電源が切断されています。
cimUpdateCompleted	CIM ファームウェアの更新処理が完了しました。
cimUpdateStarted	CIM ファームウェアの更新処理が開始しました。
configBackup	デバイス設定はバックアップされました。
configRestore	デバイス設定はリストアされました。
deviceUpdateFailed	デバイスの更新に失敗しました。
deviceUpgradeCompleted	RFP ファイルを使用した KSX II のアップデートが完了しました。
deviceUpgradeStarted	RFP ファイルを使用した KSX II のアップデートが開始されました。
ethernetFailover	Ethernet フェイルオーバが検出され、新しい Ethernet インターフェース上に復元されました。

トラップ名	説明
factoryReset	デバイスが工場出荷時のデフォルトにリセットされました。
firmwareFileDiscarded	ファームウェア ファイルが破棄されました。
firmwareUpdateFailed	ファームウェアを更新できませんでした。
firmwareValidationFailed	ファームウェアの検証に失敗しました。
groupAdded	グループが KSX II システムに追加されました。
groupDeleted	グループがシステムから削除されました。
groupModified	グループが変更されました。
ipConflictDetected	IP アドレスの競合が検出されました。
ipConflictResolved	IP アドレスの競合が解決されました。
networkFailure	製品の Ethernet インタフェースがネットワーク経由で通信できなくなりました。
networkParameterChanged	ネットワーク パラメータに変更が加えられました。
passwordSettingsChanged	強力なパスワードの設定が変更されました。
portConnect	以前認証されたユーザが KVM セッションを開始しました。
portConnectionDenied	ターゲット ポートへの接続が拒否されました。
portDisconnect	KVM セッションを実行中のユーザが正常にセッションを終了しました。
portStatusChange	ポートが使用不可能な状態になっています。
powerNotification	電源コンセントの状態の通知です。1: アクティブ、0: 非アクティブ
powerOutletNotification	電源タップ デバイスのコンセントの状態の通知です。
rebootCompleted	KSX II の再起動が完了しました。

トラップ名	説明
rebootStarted	システムへの電源の入れ直しまたは OS からのウォーム起動により、KSX II は再起動を開始しました。
securityViolation	セキュリティ違反です。
startCCManagement	デバイスが CommandCenter の管理下におかれました。
securityBannerChanged	セキュリティ バナーが変更されました。
securityBannerAction	セキュリティ バナーへのユーザの同意/拒否
setDateTime	デバイスの日時が設定されました。
setPIPSMode	デバイスの FIPS モード ステータスが変更されました。
bladeChassisCommError	このポートに接続されているブレード シャーシ デバイスで通信エラーが検出されました。
stopCCManagement	デバイスが CommandCenter の管理下から除外されました。
sxPortAlert	キーワードをログ記録し、イベントを送信します。
userAdded	ユーザ アカウントがシステムに追加されました。
userAuthenticationFailure	不正なユーザ名または/およびパスワードでのログイン試行がありました。
userConnectionLost	あるユーザのアクティブ セッションが、タイムアウトにより異常終了しました。
userDeleted	ユーザ アカウントが削除されました。
userLogin	ユーザが KSX II へ正常にログインし、認証されました。
userLogout	ユーザが KSX II から正常にログアウトしました。
userModified	ユーザ アカウントが変更されました。
userPasswordChanged	デバイスのいずれかのユーザのパスワ

トラップ名	説明
	ードが変更されると、このイベントが発生します。
userSessionTimeout	あるユーザのアクティブ セッションが、タイムアウトにより終了しました。
vmImageConnected	ユーザが仮想メディアを使用してターゲットにデバイスまたはイメージのマウントを試みました。デバイスまたはイメージのマッピング（マウント）が試行されるたびに、このイベントが生成されます。
vmImageDisconnected	ユーザが仮想メディアを使用してターゲットからデバイスまたはイメージのマウント解除を試みました。

ポートの設定

- [Port Configuration]（ポート設定）ページには、KSX II のポートの一覧が表示されます。KVM ターゲット サーバ（ブレード サーバおよび標準サーバ）およびラック PDU（電源タップ）に接続されているポートは青色で表示され、編集できます。CIM が接続されていないポート、または CIM 名が空白のポートについては、デフォルトのポート名 Dominion_KSX2_Port#が割り当てられます。「Port#」は KSX II の物理ポートの番号を表します。

- シリアル ポートに対し、シリアル ポートの [Port] (ポート) ページが開きます。

Port Configuration

▲ No.	Name	Type
1	KX-local	Not Available
2	Dominion_KSX2_Port2	Not Available
3	KX8-Local	Not Available
4	Dominion_KSX2_Port4	Not Available
5	Blade_Chassis_Port3	Not Available
6	Dominion_KSX2_Port6	Not Available
7	Dominion_KSX2_Port7	Not Available
8	Dominion_KSX2_Port8	Not Available
9	Serial Port 1	Serial
10	Serial Port 2	Serial
11	Serial Port 3	Serial
12	Serial Port 4	Serial
13	Serial Port 5	Serial
14	Serial Port 6	Serial
15	Serial Port 7	Serial
16	Serial Port 8	Serial
17	Power Port 1	PowerStrip
18	Power Port 2	PowerStrip

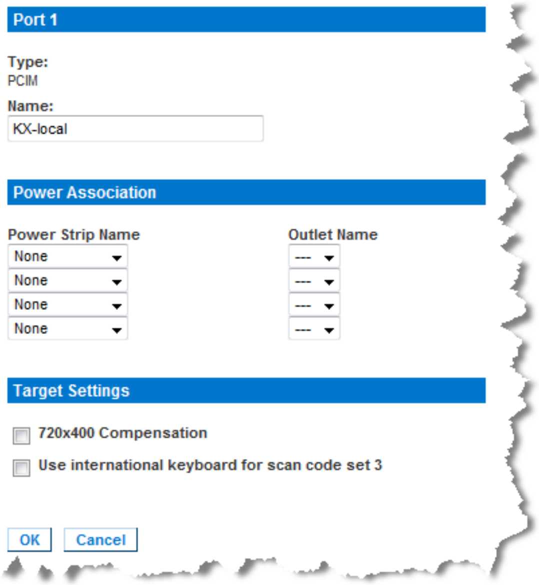
電源制御

[Port] (ポート) ページでは電源制御を構成します。[Port Configuration] (ポート設定) ページで、ターゲット サーバに接続しているポートを選択すると、[Port] (ポート) ページが開きます。

[Port] (ポート) ページで、電源の関連付けを実行したり、ポートの名前をわかりやすい名前に変更したりすることができます。

サーバには最大で 4 つの電源プラグを接続でき、それぞれに別のラック PDU (電源タップ) を関連付けられます。このページでそれらの関連付けを定義して、[Port] (ポート) ページからサーバの電源のオン、オフ、再投入を行えます。

KSX II と Dominion PX を物理的に接続する方法については、このガイドの「*E. 電源タップ* 『*32*p. の"*E. ラック PDU (電源タップ)*"参照先 』」を参照してください。



PX への名前の割り当て

[Port Configuration] (ポート設定) ページでポートを選択すると、[Port] (ポート) ページが開きます。Raritan リモート ラック PDU (電源タップ) に接続されると、このページにポートが表示されます。[Type] (タイプ) フィールドと [Name] (名前) フィールドには、あらかじめ入力されています。

このページを使用してラック PDU とそのコンセントに名前を付けます。いずれの名前にも最大 32 文字の英数字を使用でき、特殊文字を含めることができます。

注: ラック PDU がターゲット サーバ (ポート) に関連付けられると、コンセント名はターゲット サーバ名に置き換えられます (コンセントに別の名前を割り当てている場合も同様です)。

注: CommandCenter Service Gateway では、スペースを含むラック PDU 名を認識できません。

▶ ラック PDU (およびコンセント) に名前を付けるには、以下の手順に従います。

1. ラック PDU の名前を覚えやすい名前に変更します。
2. 必要に応じて、([Outlet] (コンセント)) [Name] (名前) を変更します。(デフォルトのコンセント名は、「Outlet #」です)。
3. [OK] をクリックします。

コンセントへの KVM およびシリアル ターゲット サーバの関連付け ([Port] (ポート) ページ)

サーバには最大で 4 つの電源プラグを接続でき、それぞれに別のラック PDU (電源タップ) を関連付けられます。[Port] (ポート) ページでそれらの関連付けを定義して、サーバの電源のオン、オフ、再投入を行えます。

[KVM] およびシリアルの [Port] (ポート) ページは、[Name] (名前) と [Port Association] (ポートの関連付け) セクション以外は異なります。[Power Association] (電源の関連付け) セクションは同じなので、以下の手順は、KVM およびシリアル ターゲット サーバに共通します。

▶ 電源の関連付けを行う (ラック PDU コンセントをターゲット サーバに関連付ける) には、以下の手順に従います。

注: ラック PDU がターゲット サーバ (ポート) に関連付けられると、コンセント名はターゲット サーバ名に置き換えられます (コンセントに別の名前を割り当てている場合も同様です)。

---

1. [Power Strip Name] (電源タップ名) ドロップダウン リストからラック PDU を選択します。

2. そのラック PDU に対して、[Outlet Name] (コンセント名) ドロップダウン リストからコンセントを選択します。
3. 該当するすべての電源の関連付けで、手順 1 および 2 を繰り返します。
4. [OK] をクリックします。確認メッセージが表示されます。

▶ ラック **PDU** の関連付けを削除するには、次の手順に従います。

1. [Power Strip Name] (電源タップ名) ドロップダウン リストから適切なラック PDU を選択します。
2. そのラック PDU に対して、[Outlet Name] (コンセント名) ドロップダウン リストから適切なコンセントを選択します。
3. [Outlet Name] (コンセント名) ドロップダウン リストから、[None] (設定なし) を選択します。
4. [OK] をクリックします。ラック PDU/コンセントの関連付けが削除され、確認メッセージが表示されます。

ターゲットの設定

▶ ターゲットの設定を定義するには、以下の手順に従います。

1. ターゲットの解像度が 720 x 400 のときに表示上の問題が発生する場合、[Target Settings] (ターゲット設定) セクションで [720 x 400 Compensation] (720 x 400 補正) を選択します。
2. DCIM-PS2 を使用してターゲットに接続しており、かつ、多言語キーボードでスキャン コード セット 3 を使用する必要がある場合、[Use international keyboard for scan code set 3] (多言語キーボードでスキャン コード セット 3 を使用する) を選択します。

ブレード シャーシの設定

標準型サーバとラック PDU (電源タップ) に加えて、KSX II のポートに接続されているブレード シャーシを制御することができます。一定時間に最大 8 台のブレード シャーシを管理できます。

ブレード シャーシは、ブレード シャーシ サブタイプとして設定する必要があります。ブレード シャーシ タイプがサポートされている場合、ブレード シャーシは、接続されると自動的に検出されます。シャーシ タイプがサポートされていない場合は、そのブレードを手動で設定する必要があります。

ブレード サーバ シャーシが検出された場合は、デフォルト名が関連付けられ、それが [Port Access] (ポート アクセス) ページに、標準ターゲット サーバおよびラック PDU と共に表示されます。「[Port Access] (ポート アクセス) ページ (リモート コンソール ディスプレイ)」を参照してください。

ブレード サーバは、[Port Access] (ポート アクセス) ページ上の展開可能な階層リストに表示されます。階層のルートはブレード シャーシで、個別のブレードはルートの下にラベルが付けられて表示されます。個別のブレードを表示するには、ルート シャーシの横の展開矢印アイコン ▶ を使用します。

注: ブレード シャーシを階層順に表示するには、ブレード サーバ シャーシにブレード シャーシのサブタイプを設定する必要があります。

HP ブレード シャーシおよび Cisco® UCS ブレード シャーシを除く、汎用、IBM®、Dell® の各ブレード シャーシは、[Port Access] (ポート アクセス) ページで設定されます。ブレード シャーシに接続されるポートは、ブレード シャーシ モデルで設定されている必要があります。ブレード サーバに設定できる特定の情報は、使用しているブレード サーバのブランドによって異なります。サポートされているこれらの各ブレード シャーシ固有の情報は、このセクションのヘルプにある対応するトピックを参照してください。

次のブレード シャーシがサポートされています。

- IBM BladeCenter® モデル E および H
- Dell PowerEdge® 1855、1955、および M1000e

[Generic] (汎用) オプションでは、上のリストに含まれていないブレード シャーシを設定できます。HP BladeSystem c3000 と c7000 のブレード サーバ、および Cisco UCS ブレード サーバは、Dominion デバイスから各ブレードへの個別の接続を介してサポートされます。ポートは、ポート グループ管理機能を使用して、シャーシにまとめてグループ化されます。

注: Dell PowerEdge 1855/1955 ブレードも、各個別ブレードから Dominion デバイス上のポートに接続できます。この方法で接続した場合、それらをグループ化してブレード サーバ グループを作成できます。

ブレード シャーシでは、手動設定と自動検出の 2 つの操作モードがあり、ブレード シャーシの機能によって決まります。ブレード シャーシが自動検出で設定される場合、Dominion デバイスは、以下を追跡および更新します。

- 新しいブレード サーバがいつシャーシに追加されるか。
- 既存のブレード サーバがいつシャーシから削除されるか。

注: IBM Blade Center モデル E および H を使用する場合、KSX II では、プライマリ管理モジュールとして AMM[1] の自動検出のみサポートされます。

ホット キー シーケンスを使用してブレード シャーシへの KVM アクセスを切り替えることもできます。ユーザがホットキー シーケンスを選択できるブレード シャーシの場合、これらのオプションは、[Port Configuration] (ポート設定) ページにあります。ホットキー シーケンスがあらかじめ定義されているブレード シャーシの場合、これらのシーケンスは、ブレード シャーシが選択されると [Port Configuration] (ポート設定) ページに自動的に入力されます。たとえば、IBM BladeCenter H に対する KVM を切り替えるためのデフォルト ホットキー シーケンスは、NumLock+NumLock+SlotNumber なので、設定中に IBM BladeCenter H が選択されたときに、このホットキー シーケンスがデフォルトで適用されます。ホットキー シーケンスについての詳細は、ブレード シャーシのマニュアルを参照してください。

ブレード シャーシ Web ブラウザ インタフェースがある場合は、それに対する接続を設定できます。シャーシ レベルでは、最大 4 つのリンクを定義できます。1 つ目のリンクは、ブレード シャーシ管理モジュール GUI への接続用に予約されています。たとえば、このリンクは、テクニカル サポートがシャーシ設定をすばやく検証する場合に使用されることがあります。

ブレード シャーシは、Virtual KVM Client (VKC)、Active KVM Client (AKC)、Raritan の Multi-Platform Client (MPC)、および CC-SG から管理できます。VKC、AKC、および MPC を介したブレード サーバの管理は、標準ターゲット サーバの管理と同じです。詳細は、「**ターゲット サーバの使用**」および『**CC-SG 管理者ガイド**』を参照してください。ブレード シャーシ設定に対する変更は、これらのクライアント アプリケーションに反映されます。

重要: ブレード シャーシを Dominion デバイスに CIM 接続することによって、電源がオフになったり Dominion デバイスから切断されたりした場合、ブレード シャーシに対して確立されているすべての接続が切断されます。CIM が再接続されるか電源オンにした場合は、接続を再確立する必要があります。

重要: ブレード シャーシをある Dominion デバイス ポートから別の Dominion デバイス ポートに移動する場合、CC-SG でブレード シャーシ ノードに追加されたインタフェースが CC-SG で失われます。他の情報はすべて維持されます。

汎用ブレード シャーシの設定

[Generic] (汎用) ブレード シャーシを選択した場合の操作モードは、手動設定モードだけです。 ブレード シャーシを設定する際の重要な情報および追加情報については、「サポートされているブレード シャーシ モデル」、「ブレード シャーシでサポートされている CIM」、および「*ブレード シャーシの必須および推奨設定*『*196*p. 』」を参照してください。Dell® のシャーシで KSX II を使用する場合のケーブルの長さとビデオ解像度の詳細については、「*Dell シャーシを接続する場合のケーブル長と画面解像度* 『*339*p. の"*Dell 筐体を接続する場合のケーブル長と画面解像度*"参照 』」を参照してください。

▶ シャーシを設定するには、以下の手順に従います。

1. ブレード シャーシを KSX II に接続します。装置の接続方法の詳細は、「手順 3: 装置の接続」を参照してください。
2. [Device Settings] (デバイス設定) の [Port Settings] (ポート設定) をクリックし、[Port Settings] (ポート設定) ページを開きます。
3. [Port Settings] (ポート設定) ページで、設定するブレード シャーシの名前をクリックします。[Port] (ポート) ページが開きます。
4. [Blade Chassis] (ブレード シャーシ) ラジオ ボタンを選択します。ページに、ブレード シャーシの設定に必要なフィールドが表示されます。
5. [Blade Server Chassis Model] (ブレード サーバ シャーシ モデル) ドロップダウン リストから [Generic] (汎用) を選択します。
6. ブレード シャーシを適切に設定します。
   a. [Switch Hot Key Sequence] (切り替えホットキー シーケンス) - KVM からブレード シャーシへの切り替えに使用されるホットキー シーケンスを定義します。[Switch Hot Key Sequence] (切り替えホットキー シーケンス) は、ブレード シャーシの KVM モジュールで使用されるシーケンスと同じにする必要があります。
   b. [Administrative Module Primary IP Address/Host Name] (管理モジュールのプライマリ IP アドレス/ホスト名) - 適用されません。
   c. [Maximum Number of Slots] (最大スロット数) - ブレード シャーシで使用できるデフォルトの最大スロット数を入力します。
   d. [Port Number] (ポート番号) - ブレード シャーシのデフォルトのポート番号は 22 です。 適用されません。
   e. [User Name] (ユーザ名) - 適用されません。

f. [Password] (パスワード) – 適用されません。

7. 必要に応じてブレード シャーシ名を変更します。
8. ブレードがインストールされる各スロットの横の [Installed] (インストール済み) チェックボックスをオンにして、ブレード シャーシにインストールされているブレードを指定します。または、[Select All] (すべて選択) チェックボックスをオンにします。必要な場合は、ブレード サーバ名を変更します。
9. ページの [Blade Chassis Managed Links] (ブレード シャーシ管理リンク) セクションで、ブレード シャーシ Web ブラウザ インタフェースを使用できる場合にそのインタフェースへの接続を設定できます。[Blade Chassis Managed Links] (ブレード シャーシ管理リンク) アイコン ► Blade Chassis Managed Links をクリックして、ページのセクションを展開します。

最初の URL リンクは、通常、ブレード シャーシ管理モジュール GUI への接続に使用されます。

注: ページ内のこのセクションに入力した URL リンクへのアクセスは、ブレード シャーシ ポート権限によって制御されます。

---

a. [Active] (アクティブ) – 設定されたリンクをアクティブにするには、[Active] (アクティブ) チェックボックスをオンにします。リンクを非アクティブにしておくには、チェックボックスをオフのままにします。[Active] (アクティブ) チェックボックスをオンにしていない場合でも、リンク フィールドへの情報の入力と保存はできます。[Active] (アクティブ) チェックボックスをオンにしている場合は、URL フィールドは必須です。ユーザ名、パスワード、ユーザ名フィールドおよびパスワードフィールドは、シングル サインオンを使用するかどうかに応じて、オプションになります。

b. [URL] (URL) – インタフェースへの URL を入力します。 **必ず入力してください。**

c. [Username] (ユーザ名) – インタフェースへのアクセスに使用されるユーザ名を入力します。 **(オプション)**

d. [Password] (パスワード) – インタフェースへのアクセスに使用されるパスワードを入力します。 **(オプション)**

注: DRAC、ILO、および RSA Web アプリケーションの場合は、ユーザ名とパスワードのフィールドを空白のままにしないと、接続が失敗します。

---

e. [Username Field] (ユーザ名フィールド) および [Password Field] (パスワード フィールド) は、いずれもオプションで、ユーザ名とパスワードの入力に関連付けられることが想定されたラベルが含まれています。Web アプリケーションのログイン画面で使用されるユーザ名フィールドおよびパスワード フィールドのフィールド名を入力する必要があるのはこれらのフィールドです。ログイン画面の HTML ソースを表示して、フィールド ラベルではなく、フィールドの*名前*を探すことができます。Web ブラウザ インタフェースの追加に関するヒントは、「***Web ブラウザ インタフェースの追加に関するヒント*** 『*188*p. 』」を参照してください。**(オプション)**

10. USB プロファイル情報は汎用設定には適用されません。
11. ターゲットの解像度が 720 x 400 のときに表示上の問題が発生する場合、[Target Settings] (ターゲット設定) セクションで [720 x 400 Compensation] (720 x 400 補正) を選択します。
12. DCIM-PS2 を使用してターゲットに接続しており、かつ、多言語キーボードでスキャン コード セット 3 を使用する必要がある場合、[Use international keyboard for scan code set 3] (多言語キーボードでスキャン コード セット 3 を使用する) を選択します。

CIM の本来の表示解像度を [Display Native Resolution] (本来の表示解像度) ドロップダウンから選択します。これは、デジタル CIM の優先の解像度およびタイミング モードです。解像度は、選択されたら、CIM に適用されます。

1. 選択されない場合は、デフォルトの解像度 1280 x 1024、60 Hz が使用されます。
2. [OK] をクリックして設定を保存します。

Dell ブレード シャーシの設定

ブレード シャーシを設定する際の重要な情報および追加情報については、「サポートされているブレード シャーシ モデル」、「ブレード シャーシでサポートされている CIM」、および「***ブレード シャーシの必須および推奨設定*** 『*196*p. 』」を参照してください。Dell® のシャーシで KSX II を使用する場合のケーブルの長さとビデオ解像度の詳細については、「***Dell シャーシを接続する場合のケーブル長と画面解像度*** 『*339*p. の"*Dell 筐体を接続する場合のケーブル長と画面解像度*"参照 』」を参照してください。

▶ ブレード シャーシを追加するには、以下の手順に従います。

1. ブレード シャーシを KSX II に接続します。装置の接続方法の詳細は、「手順 3: 装置の接続」を参照してください。
2. [Device Settings] (デバイス設定) の [Port Settings] (ポート設定) をクリックし、[Port Settings] (ポート設定) ページを開きます。

3. [Port Settings] (ポート設定) ページで、設定するブレード シャーシの名前をクリックします。[Port] (ポート) ページが開きます。
4. [Blade Chassis] (ブレード シャーシ) ラジオ ボタンを選択します。ページに、ブレード シャーシの設定に必要なフィールドが表示されます。
5. [Blade Server Chassis Model] (ブレード サーバ シャーシ モデル) ドロップダウン リストから Dell ブレード シャーシ モデルを選択します。

▶ Dell PowerEdge M1000e を設定するには、以下の手順に従います。

1. [Dell PowerEdge™ M1000e] (Dell PowerEdge M1000e) を選択した場合は、自動検出を使用できます。ブレード シャーシを適切に設定します。自動検出できるブレード シャーシを設定する前に、指定されたポート番号で SSH 接続を有効に設定する必要があります (「[Device Services] (デバイス サービス)」を参照してください)。また、対応する認証証明書を持つユーザ アカウントを、ブレード シャーシであらかじめ作成しておく必要があります。
   a. [Switch Hot Key Sequence] (切り替えホットキー シーケンス) - KVM からブレード サーバへの切り替えに使用されるホットキー シーケンスを選択します。 [Switch Hot Key Sequence] (切り替えホットキー シーケンス) は、ブレード シャーシの KVM モジュールで使用されるシーケンスと同じにする必要があります。
   b. [Maximum Number of Slots] (最大スロット数) - ブレード シャーシで使用できるデフォルトの最大スロット数は、自動的に入力されます。
   c. [Administrative Module Primary IP Address/Host Name] (管理モジュールのプライマリ IP アドレス/ホスト名) - ブレード シャーシのプライマリ IP アドレスを入力します。 **自動検出モードでは必須です。**
   d. [Port Number] (ポート番号) - ブレード シャーシのデフォルトのポート番号は 22 です。必要に応じて、ポート番号を変更します。**自動検出モードでは必須です。**
   e. [Username] (ユーザ名) - ブレード シャーシへのアクセスに使用されるユーザ名を入力します。 **自動検出モードでは必須です。**
   f. [Password] (パスワード) - ブレード シャーシへのアクセスに使用されるパスワードを入力します。 **自動検出モードでは必須です。**
2. KSX II でシャーシ ブレードを自動検出する場合は、[Blade Auto-Discovery] (ブレードの自動検出) チェックボックスをオンにし、[Discover Blades on Chassis Now] (ブレード シャーシを今すぐ検出) をクリックします。ブレードが検出されると、それがページに表示されます。

3. 必要に応じてブレード シャーシ名を変更します。シャーシに既に名前が付けられている場合は、その情報がこのフィールドに自動的に表示されます。まだ名前が付いていない場合は、KSX II によってシャーシに名前が割り当てられます。KSX II では、ブレード シャーシにデフォルトで「Blade_Chassis_Port#」という名前が付けられます。
4. 手動モードで操作する場合は、ブレードがインストールされる各スロットの横の [Installed] (インストール済み) チェックボックスをオンにして、ブレード シャーシにインストールされているブレードを指定します。または、[Select All] (すべて選択) チェックボックスをオンにします。必要な場合は、ブレード サーバ名を変更します。

   自動検出モードで操作する場合は、[Installed] (インストール済み) チェックボックスに、検出中にブレードを含んでいたスロットが表示されます。
5. ページの [Blade Chassis Managed Links] (ブレード シャーシ管理リンク) セクションで、ブレード シャーシ Web ブラウザ インタフェースを使用できる場合にそのインタフェースへの接続を設定できます。[Blade Chassis Managed Links] (ブレード シャーシ管理リンク) アイコン ► Blade Chassis Managed Links をクリックして、ページのセクションを展開します。

   最初の URL リンクは、通常、ブレード シャーシ管理モジュール GUI への接続に使用されます。

   注: ページ内のこのセクションに入力した URL リンクへのアクセスは、ブレード シャーシ ポート権限によって制御されます。

   ---

   a. [Active] (アクティブ) - 設定されたリンクをアクティブにするには、[Active] (アクティブ) チェックボックスをオンにします。リンクを非アクティブにしておくには、チェックボックスをオフのままにします。[Active] (アクティブ) チェックボックスをオンにしていない場合でも、リンク フィールドへの情報の入力と保存はできます。[Active] (アクティブ) チェックボックスをオンにしている場合は、URL フィールドは必須です。ユーザ名、パスワード、ユーザ名フィールドおよびパスワードフィールドは、シングル サインオンを使用するかどうかに応じて、オプションになります。
   b. [URL] (URL) - インタフェースへの URL を入力します。 Dell M1000e のサンプル設定の詳細は、「ブレード シャーシのサンプル URL フォーマット」を参照してください。
   c. [Username] (ユーザ名) - インタフェースへのアクセスに使用されるユーザ名を入力します。
   d. [Password] (パスワード) - インタフェースへのアクセスに使用されるパスワードを入力します。

注: DRAC、ILO、および RSA Web アプリケーションの場合は、ユーザ名とパスワードのフィールドを空白のまましないと、接続が失敗します。

e. [Username Field] (ユーザ名フィールド) および [Password Field] (パスワード フィールド) は、いずれもオプションで、ユーザ名とパスワードの入力に関連付けられることが想定されたラベルが含まれています。Web アプリケーションのログイン画面で使用されるユーザ名フィールドおよびパスワード フィールドのフィールド名を入力する必要があるのはこれらのフィールドです。ログイン画面の HTML ソースを表示して、フィールド ラベルではなく、フィールドの*名前*を探すことができます。Web ブラウザ インタフェースの追加に関するヒントは、「***Web ブラウザ インタフェースの追加に関するヒント*** 『*188*p. 』」を参照してください。

6. USB プロファイルは Dell シャーシには適用されません。
7. ターゲットの解像度が 720 x 400 のときに表示上の問題が発生する場合、[Target Settings] (ターゲット設定) セクションで [720 x 400 Compensation] (720 x 400 補正) を選択します。
8. DCIM-PS2 を使用してターゲットに接続しており、かつ、多言語キーボードでスキャン コード セット 3 を使用する必要がある場合、[Use international keyboard for scan code set 3] (多言語キーボードでスキャン コード セット 3 を使用する) を選択します。

CIM の本来の表示解像度を [Display Native Resolution] (本来の表示解像度) ドロップダウンから選択します。これは、デジタル CIM の優先の解像度およびタイミング モードです。解像度は、選択されたら、CIM に適用されます。

1. 選択されない場合は、デフォルトの解像度 1280 x 1024、60 Hz が使用されます。
2. [OK] をクリックして設定を保存します。

▶ Dell PowerEdge 1855/1955 を設定するには、以下の手順に従います。

1. [Dell 1855/1955] (Dell 1855/1955) を選択した場合は、自動検出は*使用できません*。ブレード シャーシを適切に設定します。

   a. [Switch Hot Key Sequence] (切り替えホットキー シーケンス) - KVM からブレード サーバへの切り替えに使用されるホットキー シーケンスを選択します。 Dell 1855/1955 モデルの場合は、KSX II によって既存のすべてのホットキー シーケンスをブロックします。汎用設定を Dell 1855 に適用する場合は、既存のホットキー 1 つだけがブロックされます。

   b. [Maximum Number of Slots] (最大スロット数) - ブレード シャーシで使用できるデフォルトの最大スロット数は、自動的に入力されます。

c. [Administrative Module Primary IP Address/Host Name] (管理モジュールのプライマリ IP アドレス/ホスト名) - 適用されません。

d. [Port Number] (ポート番号) - ブレード シャーシのデフォルトのポート番号は 22 です。 適用されません。

e. [User Name] (ユーザ名) - 適用されません。

f. [Password] (パスワード) - 適用されません。

2. 必要に応じてブレード シャーシ名を変更します。

3. ブレードがインストールされる各スロットの横の [Installed] (インストール済み) チェックボックスをオンにして、ブレード シャーシにインストールされているブレードを指定します。または、[Select All] (すべて選択) チェックボックスをオンにします。必要な場合は、ブレード サーバ名を変更します。

4. ページの [Blade Chassis Managed Links] (ブレード シャーシ管理リンク) セクションで、ブレード シャーシ Web ブラウザ インタフェースを使用できる場合にそのインタフェースへの接続を設定できます。[Blade Chassis Managed Links] (ブレード シャーシ管理リンク) アイコン ▸ Blade Chassis Managed Links をクリックして、ページのセクションを展開します。

最初の URL リンクは、通常、ブレード シャーシ管理モジュール GUI への接続に使用されます。

注: ページ内のこのセクションに入力した URL リンクへのアクセスは、ブレード シャーシ ポート権限によって制御されます。

---

a. [Active] (アクティブ) - 設定されたリンクをアクティブにするには、[Active] (アクティブ) チェックボックスをオンにします。リンクを非アクティブにしておくには、チェックボックスをオフのままにします。[Active] (アクティブ) チェックボックスをオンにしていない場合でも、リンク フィールドへの情報の入力と保存はできます。[Active] (アクティブ) チェックボックスをオンにしている場合は、URL フィールドは必須です。ユーザ名、パスワード、ユーザ名フィールドおよびパスワードフィールドは、シングル サインオンを使用するかどうかに応じて、オプションになります。

b. [URL] (URL) - インタフェースへの URL を入力します。 Dell PowerEdge 1855/1955 のサンプル設定の詳細は、「***ブレード シャーシのサンプル URL フォーマット***『*198*p. 』」を参照してください。

c. [Username] (ユーザ名) - インタフェースへのアクセスに使用されるユーザ名を入力します。

d. [Password] (パスワード) - インタフェースへのアクセスに使用されるパスワードを入力します。

注: DRAC、ILO、および RSA Web アプリケーションの場合は、ユーザ名とパスワードのフィールドを空白のまましないと、接続が失敗します。

e. [Username Field] (ユーザ名フィールド) および [Password Field] (パスワード フィールド) は、いずれもオプションで、ユーザ名とパスワードの入力に関連付けられることが想定されたラベルが含まれています。Web アプリケーションのログイン画面で使用されるユーザ名フィールドおよびパスワード フィールドのフィールド名を入力する必要があるのはこれらのフィールドです。ログイン画面の HTML ソースを表示して、フィールド ラベルではなく、フィールドの*名前*を探すことができます。Web ブラウザ インタフェースの追加に関するヒントは、「***Web ブラウザ インタフェースの追加に関するヒント*** 『*188*p. 』」を参照してください。

5. USB プロファイルは Dell シャーシには適用されません。
6. [OK] をクリックして設定を保存します。

IBM ブレード シャーシの設定

ブレード シャーシを設定する際の重要な情報および追加情報については、「サポートされているブレード シャーシ モデル」、「ブレード シャーシでサポートされている CIM」、および「***ブレード シャーシの必須および推奨設定*** 『*196*p. 』」を参照してください。Dell® のシャーシで KSX II を使用する場合のケーブルの長さとビデオ解像度の詳細については、「***Dell シャーシを接続する場合のケーブル長と画面解像度*** 『*339*p. の *"Dell 筐体を接続する場合のケーブル長と画面解像度"*参照 』」を参照してください。

▶ **ブレード シャーシを追加するには、以下の手順に従います。**

1. ブレード シャーシを KSX II に接続します。装置の接続方法の詳細は、「手順 3: 装置の接続」を参照してください。
2. [Device Settings] (デバイス設定) の [Port Settings] (ポート設定) をクリックし、[Port Settings] (ポート設定) ページを開きます。
3. [Port Settings] (ポート設定) ページで、設定するブレード シャーシの名前をクリックします。[Port] (ポート) ページが開きます。
4. [Blade Chassis] (ブレード シャーシ) ラジオ ボタンを選択します。ページに、ブレード シャーシの設定に必要なフィールドが表示されます。
5. [Blade Server Chassis Model] (ブレード サーバ シャーシ モデル) ドロップダウン リストから IBM® ブレード シャーシ モデルを選択します。

▶ IBM BladeCenter H および E を設定するには、以下の手順に従います。

1. IBM BladeCenter® H または E を選択した場合は、自動検出を使用できます。ブレード シャーシを適切に設定します。自動検出できるブレード シャーシを設定する前に、指定されたポート番号で SSH 接続を有効に設定する必要があります (「[Device Services] (デバイス サービス)」を参照してください)。また、対応する認証証明書を持つユーザ アカウントを、ブレード シャーシであらかじめ作成しておく必要があります。 KSX II では、AMM[1] の自動検出のみサポートされます。
   a. [Switch Hot Key Sequence] (切り替えホットキー シーケンス) - 定義済みです。
   b. [Maximum Number of Slots] (最大スロット数) - ブレード シャーシで使用できるデフォルトの最大スロット数は、自動的に入力されます。
   c. [Administrative Module Primary IP Address/Host Name] (管理モジュールのプライマリ IP アドレス/ホスト名) - ブレード シャーシのプライマリ IP アドレスを入力します。 **自動検出モードでは必須です。**
   d. [Port Number] (ポート番号) - ブレード シャーシのデフォルトのポート番号は 22 です。必要に応じて、ポート番号を変更します。**自動検出モードでは必須です。**
   e. [Username] (ユーザ名) - ブレード シャーシへのアクセスに使用されるユーザ名を入力します。 **自動検出モードでは必須です。**
   f. [Password] (パスワード) - ブレード シャーシへのアクセスに使用されるパスワードを入力します。 **自動検出モードでは必須です。**
2. KSX II でシャーシ ブレードを自動検出する場合は、[Blade Auto-Discovery] (ブレードの自動検出) チェックボックスをオンにし、[Discover Blades on Chassis Now] (ブレード シャーシを今すぐ検出) をクリックします。ブレードが検出されると、それがページに表示されます。
3. 必要に応じてブレード シャーシ名を変更します。シャーシに既に名前が付けられている場合は、その情報がこのフィールドに自動的に表示されます。まだ名前が付いていない場合は、KSX II によってシャーシに名前が割り当てられます。KSX II では、ブレード シャーシにデフォルトで「Blade_Chassis_Port#」という名前が付けられます。
4. 手動モードで操作する場合は、ブレードがインストールされる各スロットの横の [Installed] (インストール済み) チェックボックスをオンにして、ブレード シャーシにインストールされているブレードを指定します。または、[Select All] (すべて選択) チェックボックスをオンにします。必要な場合は、ブレード サーバ名を変更します。

自動検出モードで操作する場合は、[Installed] (インストール済み) チェックボックスに、検出中にブレードを含んでいたスロットが表示されます。

5. ページの [Blade Chassis Managed Links] (ブレード シャーシ管理リンク) セクションで、ブレード シャーシ Web ブラウザ インタフェースを使用できる場合にそのインタフェースへの接続を設定できます。[Blade Chassis Managed Links] (ブレード シャーシ管理リンク) アイコン ▶ Blade Chassis Managed Links をクリックして、ページのセクションを展開します。

   最初の URL リンクは、通常、ブレード シャーシ管理モジュール GUI への接続に使用されます。

   注: ページ内のこのセクションに入力した URL リンクへのアクセスは、ブレード シャーシ ポート権限によって制御されます。

   ---

   a. [Active] (アクティブ) – 設定されたリンクをアクティブにするには、[Active] (アクティブ) チェックボックスをオンにします。リンクを非アクティブにしておくには、チェックボックスをオフのままにします。[Active] (アクティブ) チェックボックスをオンにしていない場合でも、リンク フィールドへの情報の入力と保存はできます。[Active] (アクティブ) チェックボックスをオンにしている場合は、URL フィールドは必須です。ユーザ名、パスワード、ユーザ名フィールドおよびパスワードフィールドは、シングル サインオンを使用するかどうかに応じて、オプションになります。

   b. [URL] (URL) – インタフェースへの URL を入力します。 IBM BladeCenter のサンプル設定の詳細は、「ブレード シャーシのサンプル URL フォーマット」を参照してください。

   c. [Username] (ユーザ名) – インタフェースへのアクセスに使用されるユーザ名を入力します。

   d. [Password] (パスワード) – インタフェースへのアクセスに使用されるパスワードを入力します。

   注: DRAC、ILO、および RSA Web アプリケーションの場合は、ユーザ名とパスワードのフィールドを空白のまましないと、接続が失敗します。

   ---

e. [Username Field] (ユーザ名フィールド) および [Password Field] (パスワード フィールド) は、いずれもオプションで、ユーザ名とパスワードの入力に関連付けられることが想定されたラベルが含まれています。Web アプリケーションのログイン画面で使用されるユーザ名フィールドおよびパスワード フィールドのフィールド名を入力する必要があるのはこれらのフィールドです。ログイン画面の HTML ソースを表示して、フィールド ラベルではなく、フィールドの*名前*を探すことができます。Web ブラウザ インタフェースの追加に関するヒントは、「*Web ブラウザ インタフェースの追加に関するヒント* 『*188*p. 』」を参照してください。

6. 適用できる場合は、ブレード シャーシの USB プロファイルを定義するか、既存の USB プロファイルを選択します。[Select USB Profiles for Port] (ポートの USB プロファイルを選択) アイコン **► Select USB Profiles for Port** または [Apply Select Profiles to Other Ports] (選択したプロファイルを他のポートに適用) アイコン **► Apply Selected Profiles to Other Ports** をクリックして、ページ内のこのセクションを展開します。「*USB プロファイルの設定 ([Port] (ポート) ページ)* 『*199*p. 』」を参照してください。
7. [OK] をクリックして設定を保存します。

► IBM BladeCenter (その他) を設定するには、以下の手順に従います。

1. [IBM BladeCenter (Other)] (IBM BladeCenter (Other) を選択した場合は、自動検出は*使用できません*。ブレード シャーシを適切に設定します。
   a. [Switch Hot Key Sequence] (切り替えホットキー シーケンス) - KVM からブレード サーバへの切り替えに使用されるホットキー シーケンスを選択します。
   b. [Administrative Module Primary IP Address/Host Name] (管理モジュールのプライマリ IP アドレス/ホスト名) - ブレード シャーシのプライマリ IP アドレスを入力します。適用されません。
   c. [Maximum Number of Slots] (最大スロット数) - ブレード シャーシで使用できるデフォルトの最大スロット数を入力します。
   d. [Port Number] (ポート番号) - ブレード シャーシのデフォルトのポート番号は 22 です。 適用されません。
   e. [User Name] (ユーザ名) - 適用されません。
   f. [Password] (パスワード) - 適用されません。
2. 必要に応じてブレード シャーシ名を変更します。

3. ブレードがインストールされる各スロットの横の [Installed] (インストール済み) チェックボックスをオンにして、ブレード シャーシにインストールされているブレードを指定します。 または、[Select All] (すべて選択) チェックボックスをオンにします。必要な場合は、ブレード サーバ名を変更します。まだ名前が付いていない場合は、KSX II によってブレード サーバに名前が割り当てられます。ブレード サーバにはデフォルトで「Blade_Chassis_Port#_Slot#」という名前が付けられます。
4. ページの [Blade Chassis Managed Links] (ブレード シャーシ管理リンク) セクションで、ブレード シャーシ Web ブラウザ インタフェースを使用できる場合にそのインタフェースへの接続を設定できます。[Blade Chassis Managed Links] (ブレード シャーシ管理リンク) アイコン ► Blade Chassis Managed Links をクリックして、ページのセクションを展開します。

   最初の URL リンクは、通常、ブレード シャーシ管理モジュール GUI への接続に使用されます。

   注: ページ内のこのセクションに入力した URL リンクへのアクセスは、ブレード シャーシ ポート権限によって制御されます。

   ---

   a. [Active] (アクティブ) – 設定されたリンクをアクティブにするには、[Active] (アクティブ) チェックボックスをオンにします。リンクを非アクティブにしておくには、チェックボックスをオフのままにします。[Active] (アクティブ) チェックボックスをオンにしていない場合でも、リンク フィールドへの情報の入力と保存はできます。[Active] (アクティブ) チェックボックスをオンにしている場合は、URL フィールドは必須です。ユーザ名、パスワード、ユーザ名フィールドおよびパスワードフィールドは、シングル サインオンを使用するかどうかに応じて、オプションになります。
   b. [URL] (URL) – インタフェースへの URL を入力します。 IBM BladeCenter のサンプル設定の詳細は、「ブレード シャーシのサンプル URL フォーマット」を参照してください。
   c. [Username] (ユーザ名) – インタフェースへのアクセスに使用されるユーザ名を入力します。
   d. [Password] (パスワード) – インタフェースへのアクセスに使用されるパスワードを入力します。

   注: DRAC、ILO、および RSA Web アプリケーションの場合は、ユーザ名とパスワードのフィールドを空白のまましないと、接続が失敗します。

   ---

e. [Username Field] (ユーザ名フィールド) および [Password Field] (パスワード フィールド) は、いずれもオプションで、ユーザ名とパスワードの入力に関連付けられることが想定されたラベルが含まれています。Web アプリケーションのログイン画面で使用されるユーザ名フィールドおよびパスワード フィールドのフィールド名を入力する必要があるのはこれらのフィールドです。ログイン画面の HTML ソースを表示して、フィールド ラベルではなく、フィールドの*名前*を探すことができます。Web ブラウザ インタフェースの追加に関するヒントは、「*Web ブラウザ インタフェースの追加に関するヒント* 『*188*p. 』」を参照してください。

5. USB プロファイルは [IBM (Other)] (IBM (その他)) 設定では使用されません。
6. ターゲットの解像度が 720 x 400 のときに表示上の問題が発生する場合、[Target Settings] (ターゲット設定) セクションで [720 x 400 Compensation] (720 x 400 補正) を選択します。
7. DCIM-PS2 を使用してターゲットに接続しており、かつ、多言語キーボードでスキャン コード セット 3 を使用する必要がある場合、[Use international keyboard for scan code set 3] (多言語キーボードでスキャン コード セット 3 を使用する) を選択します。

CIM の本来の表示解像度を [Display Native Resolution] (本来の表示解像度) ドロップダウンから選択します。これは、デジタル CIM の優先の解像度およびタイミング モードです。解像度は、選択されたら、CIM に適用されます。

1. 選択されない場合は、デフォルトの解像度 1280 x 1024、60 Hz が使用されます。
2. [OK] をクリックして設定を保存します。

Web ブラウザ インタフェースの追加に関するヒント

Web ブラウザ インタフェースを追加して、埋め込み Web サーバを持つデバイスとの接続を作成できます。Web ブラウザ インタフェースは、RSA、DRAC、または ILO Processor カードに関連付けられている Web アプリケーションなどの任意の Web アプリケーションへの接続にも使用できます。

DNS を設定しておく必要があります。そうしないと、URL が解決されません。IP アドレスの場合は DNS を設定する必要はありません。

▶ Web ブラウザ インタフェースを追加するには、以下の手順に従います。

1. Web ブラウザ インタフェースのデフォルト名が提供されます。必要な場合は、[Name] (名前) フィールドで名前を変更します。

2. [URL] (URL) フィールドに Web アプリケーションの URL またはドメイン名を入力します。Web アプリケーションでユーザ名とパスワードの読み取りが行われる URL を入力する必要があります。

   正しいフォーマットについては、以下の例を参照してください。

   - http(s)://192.168.1.1/login.asp
   - http(s)://www.example.com/cgi/login
   - http(s)://example.com/home.html

3. このインタフェースへのアクセスが許可されるユーザ名とパスワードを入力します。**(オプション)**
4. ユーザ名とパスワードが入力された場合、[Username Field] (ユーザ名フィールド) と [Password Field] (パスワード フィールド) に、Web アプリケーションのログイン画面で使用されるユーザ名フィールドとパスワード フィールドのフィールド名を入力します。ログイン画面の HTML ソースを表示して、フィールド ラベルではなく、フィールドの名前を探す必要があります。

フィールド名検索に関するヒント:

- Web アプリケーションのログイン ページの HTML ソース コードで、Username や Password などのフィールドのラベルを検索します。
- フィールド ラベルが見つかったら、隣接するコードで "name="user"" のようなタグを探します。引用符内の語がフィールド名です。

HP および Cisco UCS のブレード シャーシ設定 (ポート グループ管理)

KSX II は、特定のタイプのブレードに接続されるポートをまとめてブレード シャーシを示すグループとしてサポートします。特に、Cisco® UCS ブレード、HP® BladeServer ブレード、および Dell® PowerEdge™ 1855/1955 ブレード (Dell PowerEdge 1855/1955 ブレードが個別の各ブレードから KSX II 上のポートに接続されている場合) がこれにあたります。

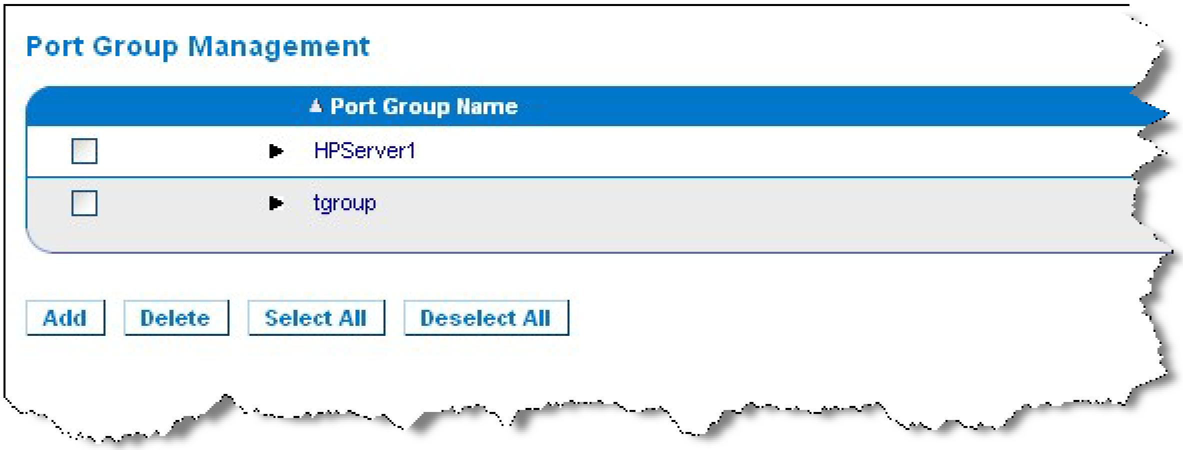
シャーシは、[Port Group Name] (ポート グループ名) によって特定され、グループは、[Port Group Management] (ポート グループ管理) ページの [Blade Server Group] (ブレード サーバ グループ) として指定されます。ポート グループには、標準 KVM ポートとして設定されたポートのみで構成され、ブレード シャーシとして設定されたポートは含まれません。ポートは、1 つのグループだけに属することができます。

ブレード シャーシで組み付けの KVM モジュールに接続されているポートは、ブレード シャーシ サブタイプとして設定されます。これらのポートは、ポート グループに含めることができます。

KSX II ポートがブレード シャーシ内で組み付けの KVM モジュールに接続され、個別のブレードに接続されていない場合、ポートはブレード シャーシ サブタイプとして設定されます。これらのポートはポート グループに含めることはできないので、[Select Port for Group] (グループ化するポートの選択) の [Available] (利用可能) リストには表示されません。

ポート グループに含まれている標準 KVM ポートを、後でブレード シャーシ サブタイプとして用途変更する場合は、まず、ポート グループからそれを削除する必要があります。

ポート グループは、[Backup and Restore] (バックアップとリストア) オプションを使用してリストアされます (「*バックアップと復元* 『*230*p. 』」を参照してください)。



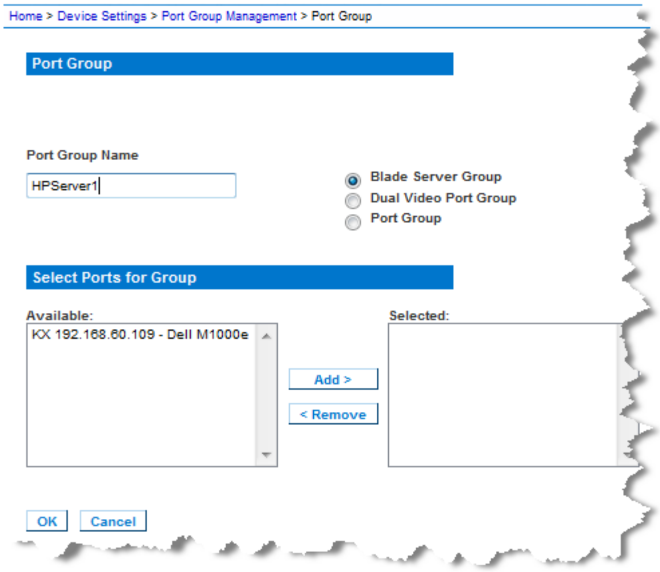
▶ ポート グループを追加するには、以下の手順に従います。

1. [Device Settings] (デバイス設定) の [Port Group Management] (ポート グループ管理) をクリックし、[Port Group Management] (ポート グループ管理) ページを開きます。
2. [Add] (追加) をクリックすると、[Port Group] (ポート グループ) ページが開きます。
3. ポート グループ名を入力します。ポート グループでは、最大 32 文字で、大文字と小文字は区別されません。
4. [Blade Server Group] (ブレード サーバ グループ) チェックボックスをオンにします。

   これらのポートをブレード シャーシ (たとえば、HP c3000 または Dell PowerEdge 1855) 内のブレードに接続するように指定する場合は、[Blade Server Group] (ブレード サーバ グループ) チェックボックスをオンにします。

   注:各ブレードは KSX II のポートに独自に接続されていますが、これは、HP ブレードをシャーシ ベースで整理する CC-SG ユーザにとっては特に重要です。

5. [Select Ports for Group] (グループ化するポートの選択) セクションの [Available] (利用可能) ボックスで、ポートをクリックします。[Add] (追加) をクリックして、ポートをグループに追加します。ポートは [Selected] (選択) ボックスに移動されます。
6. [OK] をクリックして、ポート グループを追加します。



▶ ポート グループ情報を編集するには、以下の手順に従います。

1. [Port Group Management] (ポート グループ管理) ページで、編集するポート グループのリンクをクリックします。[Port Group] (ポート グループ) ページが開きます。
2. 必要に応じて情報を編集します。
3. [OK] をクリックして変更を保存します。

▶ ポート グループを削除するには、以下の手順に従います。

1. [Port Group Management] (ポート グループ管理) ページをクリックし、削除するポート グループのチェックボックスをオンにします。
2. [Delete] (削除) をクリックします。
3. 警告メッセージで [OK] をクリックします。

サポートされているブレード シャーシ モデル

この表には、KSX II でサポートされているブレード シャーシ モデルと、それらを KSX II アプリケーションで設定する際にシャーシごとに選択する必要がある対応プロファイルが含まれています。これらのモデルのリストは、[Port Configuration] (ポート設定) ページの [Blade Server Chassis Model] (ブレード サーバ シャーシ モデル) ドロップダウン リストで選択できます。これは、[Blade Chassis] (ブレード シャーシ) ラジオ ボタンを選択している場合に表示されます。各ブレード シャーシ モデルの設定方法についての詳細は、このセクションのヘルプ内の対応するトピックを参照してください。

ブレード シャーシ モデル	KSX II プロファイル
Dell® PowerEdge™ 1855/1955	Dell PowerEdge 1855/1955
Dell PowerEdge M1000e	Dell PowerEdge M1000e
IBM® BladeCenter® S	IBM (Other)
IBM BladeCenter H	IBM BladeCenter H
IBM BladeCenter T	IBM (Other)
IBM BladeCenter HT	IBM (Other)
IBM BladeCenter E	IBM BladeCenter E
HP®	ポート グループ管理機能を使用して設定します。「*HP ブレード シャーシ設定 (ポート グループ管理)*『*190*p. の"*HP および Cisco UCS のブレード シャーシ設定 (ポート グループ管理)*"参照 』」を参照してください。

ブレード シャーシでサポートされている CIM

以下の CIM は、KSX II を通じて管理されるブレード シャーシでサポートされています。

- DCIM-PS2
- DCIM-USBG2
- D2CIM-VUSB
- D2CIM-DVUSB

以下の表に、KSX II がサポートする各ブレード シャーシ モデルでサポートされている CIM を示します。

ブレード筐体の場合	接続方法	推奨 CIM
Generic (汎用)	Generic (汎用) として設定されたブレード シャーシへの接続時に D2CIM-VUSB または D2CIM-DVUSB が使用されている場合は、[Port Configuration] (ポート設定) ページおよびクライアントの [USB Profile] (USB プロファイル) メニューから USB プロファイルを選択できます。ただし、汎用ブレード シャーシでは仮想メディアがサポートされないので、クライアントの [Virtual Media] メニューは無効になります。	• DCIM-PS2 • DCIM-USBG2
Dell® PowerEdge™ 1855	以下の 3 つの KVM モジュールのいずれかを含みます。 • アナログ KVM Ethernet スイッチ モジュール (標準) • デジタル アクセス KVM スイッチ モジュール (オプション) • KVM スイッチ モジュール (2005 年 4 月以前に販売されたシステムでの標準) これらのスイッチは、2 つの PS/2 および 1 つのビデオ デバイスをシステムに接続できるカスタム コネクタを提供します。 ソース: *Dell PowerEdge 1855 システム ユーザーズ ガイド*	• DCIM-PS2
Dell PowerEdge 1955	2 種類の KVM モジュールのいずれかがインストールされる可能性があります。 • アナログ KVM スイッチ モジュール • デジタル アクセス KVM スイッチ モジュ	• DCIM-PS2

ブレード筐体の場合	接続方法	推奨 CIM
	ール どちらのモジュールでも、PS/2 互換のキーボード、マウス、およびビデオ モニタをシステムに接続できます (システムに付属のカスタム ケーブルを使用)。 ソース: *Dell PowerEdge 1955 ハードウェア オーナーズ マニュアル*	
Dell PowerEdge M1000e	KVM スイッチ モジュール (iKVM) はこのシャーシに組み付けられています。 iKVM は、次の周辺機器に対応しています。 • USB キーボード、USB ポインティング デバイス • VGA モニタ (DDC サポート) ソース: *Dell Chassis Management Controller, Firmware Version 1.0, User Guide*	• DCIM-USBG2
HP® BladeSystem c3000	HP c-Class Blade SUV ケーブルを使用すると、ビデオと USB デバイスをサーバ ブレードに直接接続することによって、ブレード シャーシの管理、設定、および診断プロシージャを実行できます。 ソース: HP Proliant™ BL480c Server Blade Maintenance and Service Guide	• DCIM-USBG2 • D2CIM-VUSB • D2CIM-DVUSB (KVM オプションを使用しない標準 KVM ポート操作の場合)
HP BladeSystem c7000	HP c-Class Blade SUV ケーブルを使用すると、ビデオと USB デバイスをサーバ ブレードに直接接続することによって、サーバ ブレードの管理、設定、および診断プロシージャを実行できます。 ソース: *HP ProLiant BL480c Server Blade Maintenance and Service Guide*	• DCIM-USBG2 • D2CIM-VUSB • D2CIM-DVUSB (標準 KVM ポート操作)
IBM® BladeCenter® S	Advanced Management Module (AMM) は、すべてのブレード シャーシのシステム管理機能およびキーボード/ビデオ/マウス (KVM) マルチプレキシングを提供します。 AMM 接続は、シリアル ポート、ビデオ接続、リモート管理ポート (Ethernet)、およびキーボードとマウス用の 2 つの USB v2.0 ポートが含まれます。 ソース: *Implementing the IBM BladeCenter S*	• DCIM-USBG2

ブレード筐体の場合	接続方法	推奨 CIM
	Chassis	
IBM BladeCenter H	BladeCenter H シャーシには、アドバンスト マネージメント モジュールが 1 つ標準で付属しています。 ソース: *IBM BladeCenter Products and Technology*	• DCIM-USBG2 • D2CIM-DVUSB
IBM BladeCenter E	現在のモデル BladeCenter E シャーシ (8677-3Rx) には、アドバンスト マネージメント モジュールが 1 つ標準で属しています。 ソース: *IBM BladeCenter Products and Technology*	• DCIM-USBG2 • D2CIM-DVUSB
IBM BladeCenter T	BladeCenter T シャーシには、アドバンスト マネージメント モジュールが 1 つ標準で付属しています。 標準の BladeCenter シャーシとは異なり、BladeCenter T シャーシの KVM モジュールおよびマネージメント モジュールは、個別のコンポーネントになります。マネージメント モジュールの前面にあるのは、ステータスを表示する LED だけです。Ethernet および KVM 接続はすべて背面の LAN および KVM モジュールで行います。 KVM モジュールは、ホット スワップ モジュールです。シャーシの背面にキーボードとマウス用の 2 つの PS/2 コネクタ、システム ステータス パネル、および HD-15 ビデオ コネクタがあります。 ソース: *IBM BladeCenter Products and Technology*	• DCIM-PS2
IBM BladeCenter HT	BladeCenter HT シャーシには、アドバンスト マネージメント モジュールが 1 つ標準で付属しています。このモジュールは、シャーシを管理する機能とともに、ローカル KVM 機能も提供します。 ソース: *IBM BladeCenter Products and Technology*	• DCIM-USBG2

注: 自動検出をサポートするために、IBM BladeCenter モデル H および E では、ファームウェア バージョンが BPET36K 以降の AMM を使用する必要があります。

注: IBM Blade Center モデル E および H を使用する場合、KSX II では、プライマリ管理モジュールとして AMM[1] の自動検出のみサポートされます。

ブレード シャーシの必須および推奨設定

この表は、KSX II で機能させるためのブレード シャーシの設定に適用される制限についての情報を示します。以下のすべての情報に従うことをお勧めします。

ブレード シャーシの場合	必須/推奨アクション
Dell® PowerEdge™ M1000e	▪ iKVM GUI スクリーンセーバを無効にします。無効にしていない場合は、認可のダイアログが表示され、iKVM が正しく機能しません。 ▪ Dell のシャーシを Raritan CIM に接続する前に iKVM GUI メニューを終了します。終了していない場合、iKVM が正しく動作しない場合があります。 ▪ iKVM GUI の [メイン] メニューを設定して、名前ではなくスロットでターゲット ブレードを選択します。この操作を行わない場合、iKVM は正しく機能しない可能性があります。 ▪ iKVM GUI の [設定] メニューの [スキャン] でスキャン操作にスロットを*指定しないでください*。指定した場合は iKVM が正しく機能しません。 ▪ iKVM GUI の [設定] メニューの [ブロードキャスト] でキーボード/マウスのブロードキャスト操作にスロットを*指定しないでください*。指定した場合は iKVM が正しく機能しません。 ▪ iKVM GUI を呼び出す 1 つのキー シーケンスを指定します。このキー シーケンスを、KSX II でポートを設定するときにも指定する必要があります。そうしないと、クライアントのキー入力の結果として、iKVM 操作が無差別に発生する可能性があります。 ▪ Dell の CMC GUI を通じて iKVM を設定する際に、[フロントパネル USB/ビデオ有効] が*オフ*になっていることを確認します。オンになっている場合、シャーシの前面パネルでの接続が、背面の KSX II 接続よりも優先されるので、適切な iKVM 処理が行われなくなります。"User has been disabled as front panel is currently active" (フロント パネルが現在アクティブになっているのでユーザは無効です) というメッセージが表示されます。 ▪ Dell の CMC GUI を通じて iKVM を設定する際に、[iKVM から

ブレード シャーシの場合	必須/推奨アクション
	CMC CLI へのアクセスを許可する] が*オフ*になっていることを確認します。 ▪ ブレード シャーシに接続するときに iKVM GUI が表示されないようにするには、[画面遅延時間] を 8 秒に設定します。 ▪ iKVM GUI のフラグ設定中に、[時間指定] および [表示] を選択することをお勧めします。これで、目的のブレード スロットとの接続を視覚的に確認できます。
Dell PowerEdge 1855/1955	▪ iKVM GUI スクリーンセーバを無効にします。これを行わない場合は [Authorize] (認可) ダイアログ ボックスが表示され、iKVM が正しく機能しなくなります。 ▪ Dell のシャーシを Raritan CIM に接続する前に iKVM GUI メニューを終了します。終了していない場合、iKVM が正しく動作しない場合があります。 ▪ iKVM GUI の [メイン] メニューを設定して、名前ではなくスロットでターゲット ブレードを選択します。この操作を行わない場合、iKVM は正しく機能しない可能性があります。 ▪ iKVM GUI の [設定] メニューの [スキャン] でスキャン操作にスロットを*指定しないでください*。指定した場合は iKVM が正しく機能しません。 ▪ ブレード シャーシに接続するときに iKVM GUI が表示されないようにするには、[画面遅延時間] を 8 秒に設定します。 ▪ iKVM GUI のフラグ設定中に、[時間指定] および [表示] を選択することをお勧めします。これで、目的のブレード スロットとの接続を視覚的に確認できます。
IBM®/Dell® 自動検出	▪ ブレード レベルのアクセス許可を適用する場合は、自動検出を有効にすることをお勧めします。有効にしない場合は、ブレード シャーシ全体でのアクセス許可を設定します。 ▪ ブレード シャーシ管理モジュールで、Secure Shell (SSH) を有効にする必要があります。 ▪ ブレード シャーシ管理モジュールで設定された SSH ポートと、[Port Configuration] (ポート設定) ページで入力されるポート番号が一致する必要があります。
IBM 仮想メディア	▪ Raritan KSX II 仮想メディアは、IBM BladeCenter® モデル H および E でのみサポートされます。これは、D2CIM-DVUSB を使用する必要があります。黒の D2CIM-DVUSB 低速 USB コネクタは、本体背面の Administrative Management Module (AMM) に取り付けられます。グレーの D2CIM-DVUSB 高速 USB コネクタは、本体前面のメディア トレイ (MT) に取り付けられます。これには、USB 延長ケーブルが必要です。

ブレード シャーシの場合	必須/推奨アクション
Cisco® UCS サーバ シャーシ	▪ Cisco KVM ケーブル (N20-BKVM) を使用すると、ビデオと USB デバイスをサーバ ブレードに直接接続することによって、サーバ ブレードの管理、設定、および診断プロシージャを実行できます。 ▪ ソース: *Cisco UCS 5108 Server Chassis Installation Guide (DCIM-USBG2、D2CIM-VUSB、D2CIM-DVUSB)*

注:AMM を使用するすべての IBM BladeCenter では、KSX II で動作する AMM ファームウェア バージョン BPET36K 以降を使用する必要があります。

注: IBM Blade Center モデル E および H を使用する場合、KSX II では、プライマリ管理モジュールとして AMM[1] の自動検出のみサポートされます。

ブレード シャーシのサンプル URL フォーマット

この表には、KSX II で設定されるブレード シャーシのサンプル URL フォーマットが示されます。

ブレード筐体の場合	サンプル URL フォーマット
Dell® M1000e	• URL: https://192.168.60.44/cgi-bin/webcgi/login • ユーザ名: root • ユーザ名フィールド: user • パスワード: calvin • パスワード フィールド: password
Dell 1855	• URL: https://192.168.60.33/Forms/f_login • ユーザ名: root • ユーザ名フィールド: TEXT_USER_NAME • パスワード: calvin • パスワード フィールド: TEXT_PASSWORD
IBM® BladeCenter® E または H	• http://192.168.84.217/private/welcome.ssi

USB プロファイルの設定 ([Port] (ポート) ページ)

ポートで使用できる USB プロファイルを、[Port] (ポート) ページの [Select USB Profiles for Port] (ポートの USB プロファイルの選択) セクションで選択します。[Port] (ポート) ページで選択された USB プロファイルが、ポートから KVM ターゲット サーバに接続するときに VKC でユーザが使用できるプロファイルになります。デフォルト値は、Windows 2000®/Windows XP®/Windows Vista® 用のプロファイルです。USB プロファイルについての詳細は、「*USB プロファイル* 『*115*p. 』」を参照してください。

注:ポートの USB プロファイルを設定するには、デジタル CIM、VM-CIM、またはデュアル VM-CIM を、KSX II の現在のファームウェア バージョンと互換性のあるファームウェアに接続しておく必要があります。「CIM をアップグレードする」を参照してください。

ポートへの割り当てに使用できるプロファイルは、左側の [Available] (使用可能) リストに表示されます。ポートで使用するように選択したプロファイルは、右側の [Selected] (選択) リストに表示されます。いずれかのリストでプロファイルを選択した場合、プロファイルとその使用についての説明が [Profile Description] (プロファイルの説明) フィールドに表示されます。

KVM ポートで使用可能にする一連のプロファイルを選択する他に、ポートの優先プロファイルを指定して、あるポートに対する設定を他の KVM ポートに適用することもできます。

*注:DCIM-VUSB または DCIM-DVUSB 仮想メディア CIM を使用している場合、Mac OS-X® USB プロファイルの使用法については、**「*Mac のブート メニュー使用時のマウス モード *『*123*p. 』」を参照してください。*

▶ [Port] (ポート) ページを開くには、以下の手順に従います。

1. [Device Settings] (デバイス設定) の [Port Configuration] (ポート設定) を選択します。[Port Configuration] (ポート設定) ページが開きます。
2. 編集する KVM ポートの [Port Name] (ポート名) をクリックします。[Port] (ポート) ページが開きます。

▶ KVM ポートの USB ポートを選択するには、以下の手順に従います。

1. [Select USB Profiles for Port] (ポートの USB プロファイルの選択) セクションで、1 つ以上の USB プロファイルを [Available] (使用可能) リストから選択します。
   - Shift キーを押しながらクリックしてドラッグすると、複数の隣接するプロファイルを選択できます。
   - Ctrl キーを押しながらクリックすると、隣接していない複数のプロファイルを選択できます。

2. [Add] (追加) をクリックします。選択したプロファイルが [Selected] (選択) リストに表示されます。これらは、ポートに接続された KVM ターゲット サーバで使用できるプロファイルです。

▶ 優先 USB プロファイルを指定するには、以下の手順に従います。

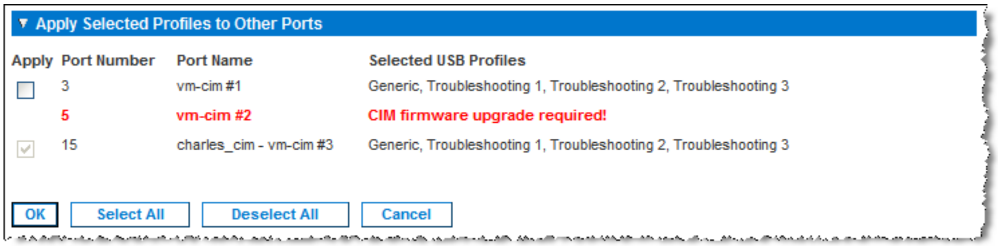
1. ポートで使用可能なプロファイルを選択した後、[Port] (ポート) メニューの [Preferred Profile] (優先プロファイル) から 1 つを選択します。デフォルトは [Generic] (汎用) です。選択したプロファイルは、KVM ターゲット サーバに接続するときに使用されます。必要に応じて、他の USB プロファイルに変更できます。
2. [Set Active Profile As Preferred Profile] (アクティブ プロファイルを優先プロファイルとして設定) チェックボックスをオンにすると、この優先 USB もアクティブ プロファイルとして使用されます。

▶ 選択した USB プロファイルを削除するには、以下の手順に従います。

1. [Select USB Profiles for Port] (ポートの USB プロファイルの選択) セクションで、1 つ以上の USB プロファイルを [Selected] (選択) リストから選択します。
   - Shift キーを押しながらクリックしてドラッグすると、複数の隣接するプロファイルを選択できます。
   - Ctrl キーを押しながらクリックすると、隣接していない複数のプロファイルを選択できます。
2. [Remove] (削除) をクリックします。選択したプロファイルが [Available] (使用可能) リストに表示されます。これらのプロファイルは、このポートに接続された KVM ターゲット サーバでは使用できなくなります。

▶ プロファイルの選択を複数のポートに適用するには、以下の手順に従います。

1. [Apply Selected Profiles to Other Ports] (選択したプロファイルを他のポートに適用) セクションで、選択した USB プロファイルの現在の設定を適用する各 KVM ポートの [Apply] (適用) チェックボックスをオンにします。



   - すべての KVM ポートを選択するには、[Select All] (すべて選択) をクリックします。

- すべての KVM ポートの選択を解除するには、[Deselect All] (すべての選択を解除) をクリックします。

KSX II のローカル ポートの設定

[Local Port Settings] (ローカル ポート設定) ページでは、KSX II ローカル コンソールに関するさまざまな設定値をカスタマイズできます。たとえば、キーボード、ホットキー、画面切り替え遅延、省電力モード、画面解像度設定、ローカル ユーザ認証などに関する設定値をカスタマイズできます。また、ローカル ポートの USB プロファイルを変更することもできます。

注:[Local Port Settings] (ローカル ポート設定) ページで設定を変更すると、作業中のブラウザが再起動する場合があります。変更時にブラウザが再起動する設定については、以下の手順に示されています。

ローカル ポートに関する設定値をカスタマイズするには

1. [Device Settings] (デバイス設定) メニューの [Local Port Settings] (ローカル ポート設定) をクリックします。[Local Port Settings] (ローカル ポート設定) ページが開きます。
2. 標準ローカル ポートを有効にするには、[Enable Standard Local Port] (標準ローカル ポートを有効にする] チェック ボックスをオンにします。無効にするにはチェックボックスをオフにします。デフォルトでは、標準ローカル ポートは有効になっていますが、必要に応じて無効にすることができます。この設定を変更すると、ブラウザが再起動します。
3. [Keyboard Type] (キーボード タイプ) ボックスの一覧でキーボード タイプを選択します。選択できる項目は次のとおりです。この設定を変更すると、ブラウザが再起動します。
   - [US] (アメリカ英語)
   - [US/International] (アメリカ英語/国際)
   - [United Kingdom] (イギリス英語)
   - [French (France)] (フランス語 (フランス))
   - [German (Germany)] (ドイツ語 (ドイツ))
   - [JIS (Japanese Industry Standard)] (JIS (日本工業規格))
   - [Simplified Chinese] (簡体字中国語)
   - [Traditional Chinese] (繁体字中国語)
   - [Dubeolsik Hangul (Korean)] (Dubeolsik ハングル (韓国))
   - [German (Switzerland)] (ドイツ語 (スイス))
   - [Portuguese (Portugal)] (ポルトガル語 (ポルトガル))
   - [Norwegian (Norway)] (ノルウェー語 (ノルウェー))
   - [Swedish (Sweden)] (スウェーデン語 (スウェーデン))
   - [Danish (Denmark)] (デンマーク語 (デンマーク))

- [Belgian (Belgium)] (ベルギー語 (ベルギー))

注: 中国語、日本語、および韓国語は、表示しかできません。現時点では、これらの言語を入力することはできません。

注: トルコ語のキーボードを使用している場合は、Active KVM Client (AKC) を介してターゲット サーバに接続する必要があります。他の Raritan クライアントではサポートされていません。

---

4. [Local Port Hotkey] (ローカル ポート ホットキー) ボックスの一覧でローカル ポート ホットキーを選択します。ローカル ポート ホットキーは、ターゲット サーバの画面が表示されているときに KSX II ローカル コンソールの画面に戻す際に使用します。デフォルト値は [Double Click Scroll Lock] (Scroll Lock キーを 2 回押す) ですが、他のキー組み合わせを選択することもできます。

ホットキー	説明
Scroll Lock キーをすばやく 2 回押す	Scroll Lock キーをすばやく 2 回押します。
[Double Click Num Lock] (Num Lock キーを 2 回押す)	Num Lock キーをすばやく 2 回押します。
[Double Click Caps Lock] (Caps Lock キーを 2 回押す)	Caps Lock キーをすばやく 2 回押します。
[Double Click Left Alt key] (左 Alt キーを 2 回押す)	左 Alt キーをすばやく 2 回押します。
[Double Click Left Shift key] (左 Shift キーを 2 回押す)	左 Shift キーをすばやく 2 回押します。
[Double Click Left Ctrl key] (左 Ctrl キーを 2 回押す)	左 Ctrl キーをすばやく 2 回押します。

5. ローカル ポート接続キーを選択します。接続キーは、あるターゲット サーバにアクセスしているときに別のターゲット サーバに切り替える際に使用します。

   その後ホットキーを使用して、そのターゲット サーバの画面から KSX II ローカル コンソールの画面に戻すことができます。

   接続キーを設定すると、ナビゲーション パネルに表示されるので、すぐにわかります。接続キー組み合わせの例については、「***接続キーの例*** 『*273*p. 』」を参照してください。
6. 接続キーは、標準型サーバとブレード筐体のどちらに対しても機能します。

7. 必要に応じて、[画面切り替え遅延(秒)] ボックスに 0 ～ 5 秒の範囲の数値を入力します。通常は「0」と入力します。ただし、一部のモニタでは画面切り替えに時間がかかるので、その場合は適切な値を入力します。
8. 省電力機能を利用する場合、次の手順を実行します。
   a. [省電力モード] チェック ボックスをオンにします。
   b. [省電力モードのタイムアウト (分)] ボックスに、省電力モードに移行するまでの時間 (単位: 分) を入力します。
9. [解像度] ボックスの一覧で、KSX II ローカル コンソールの画面解像度を選択します。選択できる項目は次のとおりです。この設定を変更すると、ブラウザが再起動します。
   - 800 x 600
   - 1024 x 768
   - 1280 x 1024
10. [垂直走査周波数 (Hz)] ボックスの一覧で垂直走査周波数を選択します。選択できる項目は次のとおりです。この設定を変更すると、ブラウザが再起動します。
   - 60 Hz
   - 75 Hz
11. [ローカル ユーザ認証] でローカル ユーザ認証タイプを選択します。
   - [ローカル/LDAP/RADIUS]: これは推奨オプションです。認証の詳細については、「***リモート認証*** 『*41*p. 』」を参照してください。
   - [なし]: KSX II ローカル コンソールからのアクセスに対して認証は行われません。このオプションは、安全な環境でのみ選択することをお勧めします。
   - KSX II が CommandCenter Secure Gateway (CC-SG) の管理下にある場合にローカル ユーザを認証するには、[Ignore CC managed mode on local port] (ローカル ポートからのアクセスを CC-SG の管理対象から除外する) チェック ボックスをオンにします。

注: 最初は [Ignore CC managed mode on local port] (ローカル ポートからのアクセスを CC-SG の管理対象から除外する) チェック ボックスをオフにしていたが、後でローカル ポートからのアクセスを CC-SG の管理対象から除外したくなった場合、CC-SG 側で KSX II を CC-SG の管理対象から除外する必要があります。その後、[Ignore CC managed mode on local port] (ローカル ポートからのアクセスを CC-SG の管理対象から除外する) チェック ボックスをオンにすることができます。

---

12. [OK] をクリックします。

ポート キーワード

ポート キーワードはフィルタとして機能します。キーワードが検出されると、そのキーワードを含むメッセージがローカル ポート ログに記録され、対応するトラップが SNMP を介して送信されます (設定されている場合)。

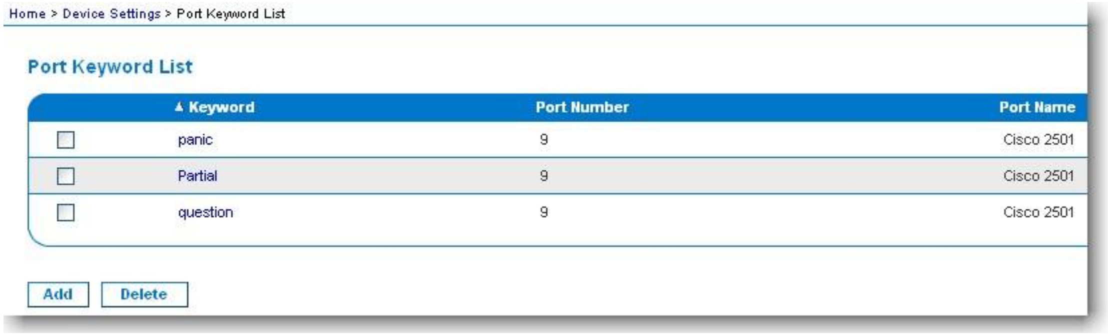
キーワードを定義すると、ローカル ポートに記録されるのはそのキーワードを含むメッセージのみになります。

ポート キーワードを作成し、以下と関連付けることができます。

- Syslog
- 監査ログ
- SNMP トラップ

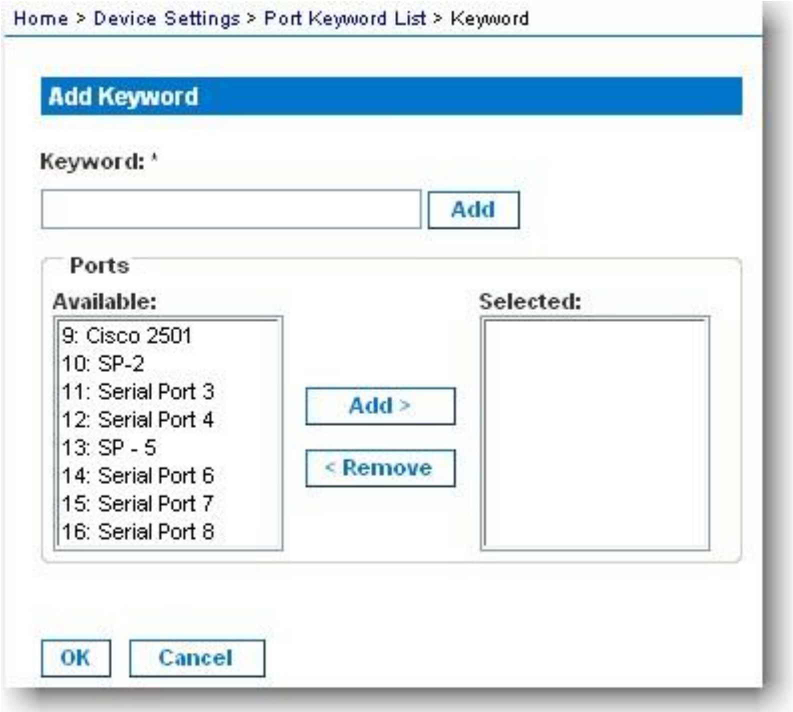
▶ **キーワードを定義してポートと関連付けるには、以下の手順に従います。**

1. [Device Settings] (デバイスの設定)、[Port Keyword List] (ポート キーワードのリスト)、[Keyword] (キーワード) を選択します。[Port Keyword List] (ポート キーワードのリスト) ページが開きます。



キーワードがまだ作成されていない場合は、このページに「*There are no port keywords defined (ポート キーワードが定義されていません)*」というメッセージが表示されます。ポート キーワードが存在する場合、それらのキーワードが [Port Keyword List] (ポート キーワード リスト) ページに表示されます。

2. 初めてキーワードを定義する場合は、[Port Keyword List] (ポート キーワード リスト) ページで [Add] (追加) ボタンをクリックします。[Add Keyword] (キーワードの追加) ページが開きます。新しいキーワードを作成するには、手順 3 〜 5 に従います。



3. [Keyword] (キーワード) フィールドにキーワードを入力し、[Add] (追加) ボタンをクリックします。キーワードは、[Keyword] (キーワード) フィールド配下のページに直接追加され、[OK] を選択することで [Port Keyword List] (ポート キーワード リスト) ページに表示されます。必要に応じて同じ手順を繰り返して、キーワードを追加してください。
4. このページの [Ports] (ポート) セクションにある [Available] (使用可能) 選択ボックスで、そのキーワードと関連付けるポートを 1 つまたは複数クリックし、[Add] (追加) をクリックします。キーワードと関連付けられたポートが、[Selected] (選択) 選択ボックスに移動します。必要に応じて、ポートの追加を続けます。
5. [OK] をクリックします。

▶ 選択リストからポートを削除するには、以下の手順に従います。

1. [Add Keyword] (キーワードの追加) ページで、[Selected] (選択) 選択ボックス内のポートをクリックし、[Remove] (削除) をクリックします。

- **キーワードを削除するには、以下の手順に従います。**

1. [Port Keyword List] (ポート キーワード リスト) ページで、削除するキーワードのチェックボックスをオンにします。
2. [Delete] (削除) ボタンをクリックします。警告メッセージが表示されます。
3. 警告メッセージの [OK] をクリックします。

ポート グループ管理

この機能は、HP ブレード シャーシ構成固有のものです。「*HP ブレード シャーシ設定 (ポート グループ管理)* 『*190*p. の"*HP および Cisco UCS のブレード シャーシ設定 (ポート グループ管理)*"参照 』」を参照してください。

Ch 9　セキュリティの管理

この章の内容

セキュリティの設定 207
IP アクセス制御を設定する 219
SSL 証明書 221
セキュリティ バナー 224

セキュリティの設定

[Security Settings] (セキュリティ設定) ページで、ログオン制限、ユーザ ブロック、パスワード ルール、および暗号化と共有に関する設定を行うことができます。

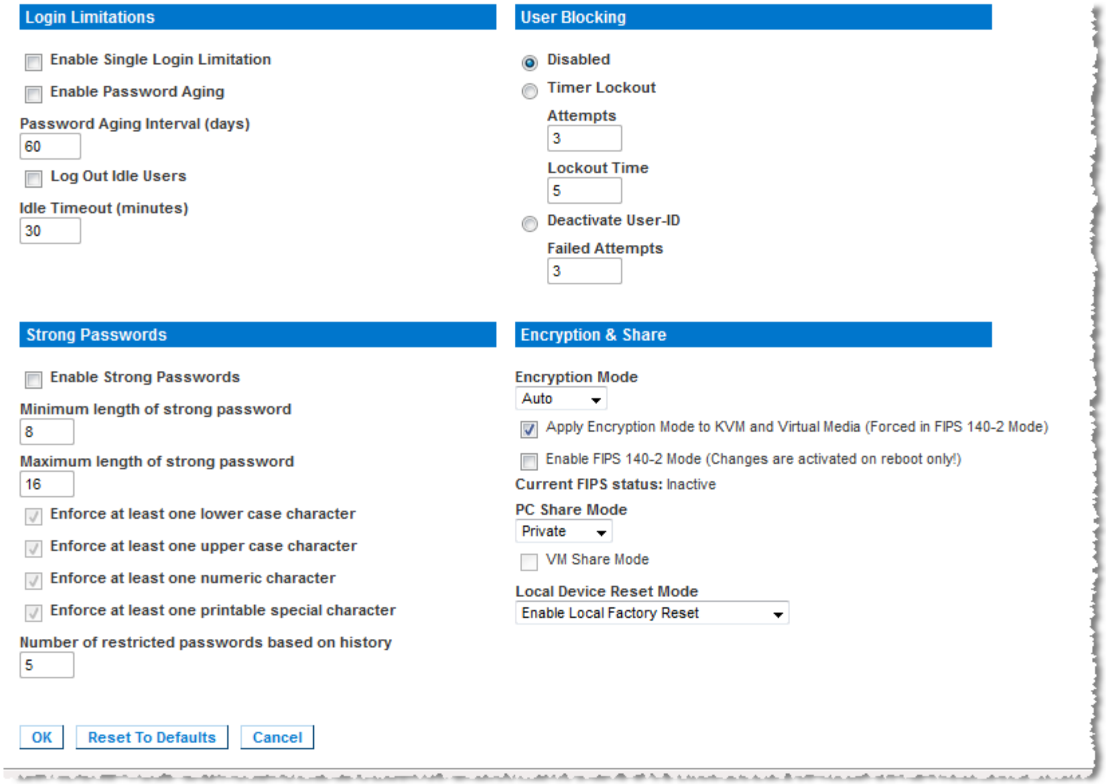
パブリック キーとプライベート キーの交換には Raritan SSL 証明書が使用され、セキュリティのレベルを高めます。Raritan の Web サーバ証明書は自己署名されています。Java アプレット証明書は、VeriSign の証明書によって署名されています。暗号化によって、情報が漏洩しないよう保護されていることが保証されます。また、これらの証明書によって、団体の身元が Raritan, Inc であることが立証されます。

▶ セキュリティ設定を行うには、以下の手順に従います。

1. [Security] (セキュリティ) の [Security Settings] (セキュリティ設定) を選択します。[Security Settings] (セキュリティ設定) ページが開きます。
2. 必要に応じて、*[Login Limitations] (ログイン制限)* 『*208*p. 』 の設定を更新します。
3. 必要に応じて、*[Strong Passwords] (強力なパスワード)* 『*210*p. 』 の設定を更新します。
4. 必要に応じて、*[User Blocking] (ユーザ ブロック)* 『*211*p. の"*[ユーザ ブロック]*"参照 』 の設定を更新します。
5. 必要に応じて、[Encryption & Share] (暗号化および共有) の設定を更新します。
6. [OK] をクリックします。

▶ デフォルトに戻すには、以下の手順に従います。

- [Reset to Defaults] (デフォルトに戻す) をクリックします。

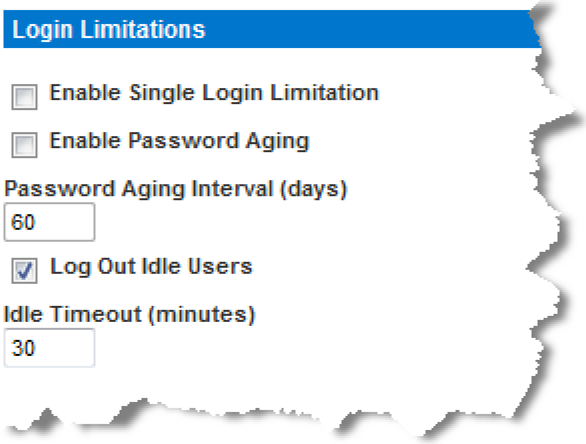


[Login Limitations] (ログイン制限)

ログイン制限を使用して、シングル ログイン、パスワード エージング、アイドル ユーザのログアウトに関する制限を指定できます。

制限	説明
[Enable Single Login Limitation] (シングル ログイン制限を有効にする)	これを選択すると、常時ユーザ名ごとに 1 人のログインしか許可されません。このチェック ボックスをオフにした場合、所定のユーザ名とパスワードの組み合わせで、複数のクライアント ワークステーションからデバイスに同時接続できます。
[Enable password aging] (パスワード エージングを有効にする)	これを選択すると、[Password Aging Interval] (パスワード エージング間隔) フィールドで指定した日数に基づいて、すべてのユーザに対して定期的にパスワードを変更するよう要求します。 [Enable Password Aging] (パスワード エージング

制限	説明
	を有効にする）チェックボックスをオンにするとこのフィールドが有効になるため、設定する必要があります。パスワードの変更が要求される間隔を日数で入力します。デフォルトの日数は 60 日です。
[Log out idle users]（アイドル ユーザのログアウト）、[After (1-365 minutes)]（経過時間（1 ～ 365 分））	[Log out idle users]（アイドル ユーザのログアウト）チェックボックスをオンにして、[After (1-365 minutes)]（経過時間（1 ～ 365 分））フィールドで指定した時間の経過後にユーザを自動的に切断します。キーボードまたはマウスで操作が行われない場合は、すべての セッションおよびすべてのリソースがログアウトされます。ただし、実行中の仮想メディア セッションはタイムアウトしません。 [After]（経過時間）フィールドは、アイドル ユーザがログアウトされるまでの時間（分）を設定するために使用されます。このボックスが有効になるのは、[Log Out Idle Users]（アイドル ユーザをログオフする）チェック ボックスをオンにした場合です。フィールド値として最大 365 分を入力できます。



[Strong Passwords] (強力なパスワード)

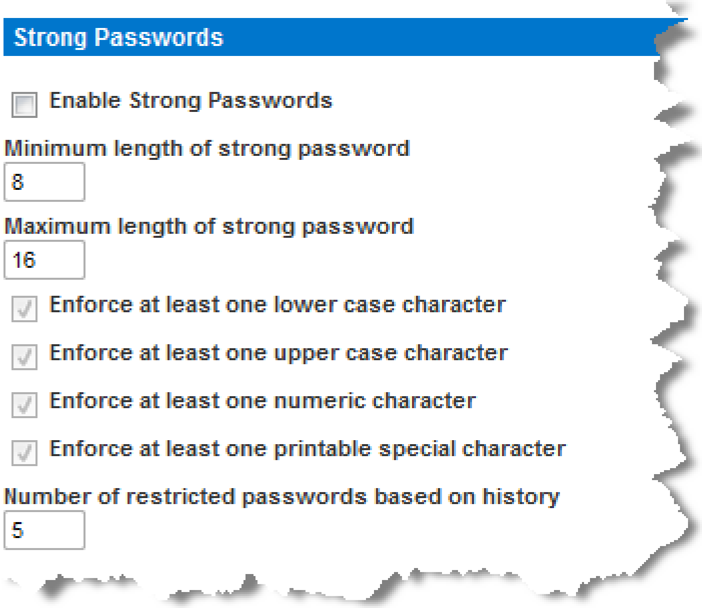
[Strong Passwords] (強力なパスワード) セクションで値を指定すると、このシステムにおけるローカル認証の安全性が高まります。強力なパスワードを使用すると、最小長と最大長、必要な文字、パスワード履歴の保持など、有効な KSX II ローカル パスワードの形式を指定できます。

強力なパスワードには、アルファベットとアルファベット以外の文字 (句読点または数字) をそれぞれ 1 文字以上含むパスワードを指定する必要があります。また、パスワードとユーザ名の最初の 4 文字には同じ文字列を使用できません。

これを選択すると、強力なパスワードのルールが適用されます。パスワードが強力なパスワードの基準を満たしていない場合、ユーザは次回ログオンする際にパスワードを変更するよう自動的に求められます。[Enable Strong Passwords] (強力なパスワードを有効にする) チェック ボックスをオフにした場合、標準の形式になっているかどうかだけが検査されます。[Enable Strong Passwords] (強力なパスワードを有効にする) チェック ボックスをオンにした場合、次のフィールドが有効になるので、指定する必要があります。

フィールド	説明
[Minimum length of strong password] (強力なパスワードの最小長)	パスワードは 8 文字以上でなければなりません。デフォルトでは 8 文字ですが、管理者は最小長を 63 文字に変更することができます。
[Maximum length of strong password] (強力なパスワードの最大長)	デフォルトの最小長は 8 文字ですが、管理者は最大長をデフォルトの 16 文字に設定することができます。強力なパスワードの最大長は 63 文字です。
[Enforce at least one lower case character] (1 文字以上の小文字の使用を強制する)	これを選択すると、パスワードに 1 文字以上の小文字が必要になります。
[Enforce at least one upper case character] (1 文字以上の大文字の使用を強制する)	これを選択すると、パスワードに 1 文字以上の大文字が必要になります。
[Enforce at least one numeric character] (1 文字以上の数字の使用を強制する)	これを選択すると、パスワードに 1 文字以上の数字が必要になります。
[Enforce at least one printable special character] (1 文字以上の印刷可能な特殊文字の使用を強制する)	これを選択すると、パスワードに 1 文字以上の印刷可能な特殊文字が必要になります。

フィールド	説明
[Number of restricted passwords based on history] (履歴に基づく制限パスワードの数)	このフィールドは、パスワード履歴数を表します。つまり、繰り返し使用できない以前のパスワードの数を表します。範囲は 1 ～ 12 で、デフォルトは 5 です。



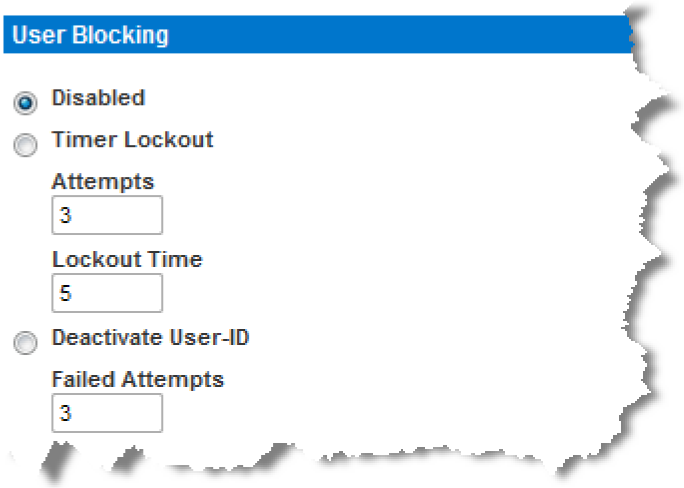
[ユーザ ブロック]

[ユーザ ブロック] セクションでは基準を指定し、ユーザが指定回数ログオンに失敗するとシステムにアクセスできなくなるようにします。

次の 3 つのオプションは、相互に排他的です。

オプション	説明
[無効]	デフォルト値です。認証に失敗した回数に関わらず、ユーザのアクセスはブロックされません。

<table>
<tr><th>オプション</th><th>説明</th></tr>
<tr><td>[タイマ ロックアウト]</td><td>ユーザが指定回数より多くログオンに失敗すると、システムへのアクセスが指定の時間拒否されます。これを選択した場合は次のフィールドが有効になります。
[試行回数]: この回数より多くログオンに失敗すると、ユーザはロックアウトされます。有効な範囲は 1 ～ 10 で、デフォルトの試行回数は 3 です。
[ロックアウト時間]: ユーザがロックアウトされる時間です。有効な範囲は 1 ～ 1440 分で、デフォルトでは 5 分です。
注: [タイマ ロックアウト] で指定した値は、Administrator の役割が割り当てられているユーザには適用されません。</td></tr>
<tr><td>[ユーザ ID を無効化]</td><td>このオプションを選択した場合は、[試行回数] フィールドで指定した回数より多くログオンに失敗すると、ユーザはシステムからロックアウトされます。
[試行回数]: この回数より多くログオンに失敗すると、そのユーザのユーザ ID が無効になります。このボックスが有効になるのは、[ユーザ ID を無効化] オプションを選択した場合です。有効な範囲は 1 ～ 10 です。
指定回数より多くログオンに失敗してユーザ ID が無効になった場合、管理者はユーザ パスワードを変更し、[ユーザ] ページの [有効化] チェックボックスをオンにしてユーザ アカウントを有効化する必要があります。</td></tr>
</table>



[Encryption & Share] (暗号化および共有)

[Encryption & Share] (暗号化および共有) セクションでは、使用する暗号化のタイプ、PC と VM の共有モード、KSX II のリセット ボタンを押したときに実行されるリセットのタイプを指定できます。

> 警告: ご使用のブラウザでサポートされていない暗号化モードを選択した場合、そのブラウザから KSX II にアクセスできなくなります。

▶ 暗号化および共有を設定するには、以下の手順に従います。

1. [Encryption Mode] (暗号化モード) ドロップダウン リストからオプションのいずれかを選択します。

   暗号化モードを選択しても、使用しているブラウザで、選択したモードがサポートされていない場合は、KSX II に接続できないという警告が表示されます。警告「When the Encryption Mode is specified please ensure that your browser supports this encryption mode; otherwise you will not be able to connect to the ProductName. ([Encryption Mode] (暗号化モード) が指定されている場合は、ブラウザでこの暗号化モードがサポートされていることを確認してください。サポートされていない場合は、KSX II に接続できません。)」が表示されます。

暗号化モード	説明
自動	推奨のオプションです。KSX II で、自動ネゴシエーションによって考えられる最高の暗号化レベルに設定されます。 デバイスとクライアントが FIPS 準拠アルゴリズムの使用を正常にネゴシエートできるようにするには、[Auot] (自動) を選択する必要があります。

暗号化モード	説明
[RC4] (RC4)	RSA RC4 暗号方式を使用して、ユーザ名、パスワード、ビデオ送信を含む KVM データが保護されます。これは、最初の接続認証中に KSX II デバイスとリモート PC 間のプライベート通信チャンネルを提供する 128 ビットの SSL (セキュア ソケット レイヤ) プロトコルです。 FIPS 140-2 モードを有効にして [RC4] (RC4) を選択すると、エラー メッセージが表示されます。[RC4] (RC4) は FIPS 140-2 モードでは使用できません。
[AES-128]	AES (Advanced Encryption Standard) は、電子データの暗号化に関するアメリカの国立標準技術研究所の仕様です。128 はキーの長さを表します。[AES-128] (AES-256) を指定した場合は、使用しているブラウザで AES がサポートされていることを確認してください。サポートされていない場合は、接続できません。詳細については、「*Checking Your Browser for AES Encryption (使用しているブラウザの AES 暗号化を確認する)*『*216*p. の"*ご使用のブラウザで AES 暗号化方式がサポートされているかどうかを確認する*"参照 』」を参照してください。
[AES-256]	AES (Advanced Encryption Standard) は、電子データの暗号化に関するアメリカの国立標準技術研究所の仕様です。256 はキーの長さを表します。[AES-256] (AES-256) を指定した場合は、使用しているブラウザで AES がサポートされていることを確認してください。サポートされていない場合は、接続できません。詳細については、「*Checking Your Browser for AES Encryption (使用しているブラウザの AES 暗号化を確認する)*『*216*p. の"*ご使用のブラウザで AES 暗号化方式がサポートされているかどうかを確認する*"参照 』」を参照してください。

注: [自動] を選択しなかった場合、MPC は最高強度の暗号化モードに設定されます。

注: Windows XP® (Service Pack 2 適用) と Internet Explorer® 7 を使用している場合、AES-128 暗号化モードで KSX II にリモート接続することはできません。

2. [Apply Encryption Mode to KVM and Virtual Media] (暗号化モードを KVM および仮想メディアに適用する) チェック ボックスの値を指定します。このチェック ボックスをオンにした場合、選択した暗号化モードが KVM と仮想メディアの両方に適用されます。認証後、KVM データと仮想メディア データが 128 ビットの暗号化モードで転送されます。
3. 政府やその他のセキュリティの高い環境では、[Enable FIPS 140-2] (FIPS 140-2 を有効にする) チェックボックスをオンにして FIPS 140-2 モードを有効にします。FIPS 140-2 を有効にする方法については、「*FIPS 140-2 の有効化* 『*217*p. 』」を参照してください。
4. [PC Share Mode] (PC 共有モード) - グローバルな同時リモート KVM アクセスを特定し、最大 8 人までのリモート ユーザが KSX II に同時にログオンし、デバイスを介してターゲット サーバを同時に表示および制御できるようにします。次のいずれかのオプションを選択します。
   - [Private] (プライベート): PC を共有しません。これはデフォルト値です。一度に 1 人のユーザが、排他的に各ターゲット サーバにアクセスできます。
   - [PC-Share] (PC 共有): KVM ターゲット サーバに最大 8 人のユーザ (管理者または非管理者) が同時にアクセスできます。ただし、リモート ユーザはキーボートやマウスで全く同じ操作を行えるため、文字の入力やマウスの操作を止めないユーザがいると、制御が不規則になる場合があることに注意してください。
5. 必要に応じて、[VM Share Mode] (VM 共有モード) チェック ボックスをオンにします。このチェック ボックスは [PC-Share Mode] (PC 共有モード) ボックスの一覧で [PC-Share] (PC 共有) を選択した場合にのみ有効になります。このオプションを選択すると、複数のユーザで仮想メディアを共有できるようになります。つまり、複数のユーザが同じ仮想メディア セッションにアクセスできます。デフォルトでは、このチェック ボックスはオフになっています。
6. 必要に応じて、[Local Device Reset Mode] (ローカル デバイス リセット モード) ボックスの一覧で値を選択します。このオプションでは、ユニットの背面にあるハードウェア リセット ボタンが押下された際に実行するアクションを指定します。詳細については、「リセット ボタンを使用して KSX II をリセットする」を参照してください。次のいずれかの値を選択します。

ローカル デバイス リセット モード	説明
[Enable Local Factory	KSX II を出荷時設定にリセットします。

ローカル デバイス リセット モード	説明
Reset] (ローカルで出荷時設定にリセットする) (デフォルト)	
[Enable Local Admin Password Reset] (ローカルで管理者パスワードだけをリセットする)	ローカルの管理者パスワードだけをリセットします。パスワードは raritan に戻ります。
[Disable All Local Resets] (ローカルでリセットしない)	リセットは一切実行されません。

注: P2CIM-AUSBDUAL または P2CIM-APS2DUAL を使用してターゲットを 2 台の KSX II に接続しており、かつ、ターゲットへのプライベート アクセスが必要である場合、両方の KSX II において PC 共有モードを [Private] (プライベート) に設定する必要があります。

Paragon CIM と ProductName を組み合わせて使用する場合の詳細については、「***サポートされている Paragon CIM および設定*** 『***303***p. の"***サポートされている Paragon II CIMS および設定***"参照 』」を参照してください。

ご使用のブラウザで AES 暗号化方式がサポートされているかどうかを確認する

ブラウザで AES が使用されているかどうかわからない場合は、ブラウザの製造元に問い合わせるか、暗号化方法を調べたいブラウザを使用して https://www.fortify.net/sslcheck.html Web サイトにアクセスしてください。この Web サイトでは、ブラウザの暗号化方法が検出され、レポートが表示されます。

AES 256 ビット暗号化方式は、以下のブラウザでサポートされています。

- Firefox®
- Internet Explorer®

AES 256 ビット暗号化方式を使用するには、サポート対象ブラウザを使用することに加え、Java™ Cryptography Extension® (JCE®) 無制限強度の管轄ポリシー ファイルをインストールする必要があります。

各種 JRE™ の管轄ファイルは、次のページの [other downloads] セクションで入手できます。

- JRE1.7 - javase/downloads/jce-7-download-432124.html

FIPS 140-2 の有効化

政府やその他のセキュリティの高い環境では、場合によっては、FIPS 140-2 モードを有効にする必要があります。

KSX II では、『FIPS 140-2 Implementation Guidance』(FIPS 140-2 実装ガイダンス) の G.5 セクションのガイドラインに従って、Linux® プラットフォームで実行されている FIPS 140-2 で検証された埋め込み暗号化モジュールが使用されます。

このモードを有効にすると、SSL 証明書の生成に使用される秘密鍵を内部で生成する必要があり、ダウンロードしたりエクスポートしたりすることはできません。

FIPS 140-2 モードを有効にすると、パフォーマンスが低下する場合があります。

▶ FIPS 140-2 を有効にするには、以下の手順に従います。

1. [Security Settings] (セキュリティ設定) ページを開きます。
2. [Security Settings] (セキュリティ設定) ページの [Encryption & Share] (暗号化および共有) セクションで [Enable FIPS 140-2] (FIPS 140-2 を有効にする) チェックボックスをオンにして、FIPS 140-2 モードを有効にします。

   FIPS 140-2 モードでは、外部通信に FIPS 140-2 で承認されたアルゴリズムを利用します。

   ビデオ、キーボード、マウス、仮想メディア、およびスマート カードのデータで構成される KVM セッション トラフィックの暗号化には、FIPS 暗号化モジュールが使用されます。

3. KSX II を再起動します。Required

   FIPS モードが有効になると、「FIPS Mode: Enabled」(FIPS モード: 有効) というメッセージが画面の左パネルの [Device Information] (デバイス情報) セクションに表示されます。

   FIPS モードが有効になったら、セキュリティを強化するために、新しい証明書署名要求を作成することもできます。この要求は、必要な鍵暗号を使用して作成されます。署名された証明書をアップロードするか、自己署名証明書を作成します。SSL 証明書の状態は、[Not FIPS Mode Compliant] (FIPS モード非準拠) から [FIPS Mode Compliant] (FIPS モード準拠) に更新されます。

   FIPS モードが有効になっている場合は、鍵ファイルをダウンロードまたはアップロードできません。最後に作成された CSR が内部で鍵ファイルに関連付けられます。さらに、CA からの SSL 証明書とその秘密鍵は、バックアップされたファイルの完全な復元に含まれません。鍵を KSX II からエクスポートすることはできません。

FIPS 140-2 サポートの要件

KSX II では、FIPS 140-2 で承認された暗号化アルゴリズムの使用がサポートされます。これにより、クライアントが FIPS 140-2 専用モードに設定されている場合に、SSL サーバとクライアントでは、暗号化されたセッションに使用されている暗号スイートを正常にネゴシエートできます。

KSX II で FIPS 140-2 を使用する場合の推奨事項を以下に示します。

KSX II

- [Security Settings] (セキュリティ設定) ページで、[Encryption & Share] (暗号化および共有) を [Auto] (自動) に設定します。「*暗号化および共有* 『*213*p. の"*[Encryption & Share] (暗号化および共有)*"参照 』」を参照してください。

Microsoft クライアント

- クライアント コンピュータと Internet Explorer で FIPS 140-2 を有効にする必要があります。

Windows クライアントで FIPS 140-2 を有効にするには、以下の手順に従います。

1. [コントロール パネル]、[管理ツール]、[ローカル セキュリティ ポリシー] の順に選択して、[ローカル セキュリティ設定] ダイアログ ボックスを開きます。
2. ナビゲーション ツリーで、[ローカル ポリシー]、[セキュリティ オプション] の順に選択します。
3. [システム暗号化: 暗号化、ハッシュ、署名のための FIPS 準拠アルゴリズムを使う] を有効にします。
4. クライアント コンピュータを再起動します。

Internet Explorer で FIPS 140-2 を有効にするには、以下の手順に従います。

1. Internet Explorer で、[ツール] の [インターネット オプション] を選択し、[詳細設定] タブをクリックします。
2. [TLS 1.0 を使用する] チェックボックスをオンにします。
3. ブラウザを再起動します。

IP アクセス制御を設定する

IP アクセス制御機能を利用することにより、KSX II に対するアクセスを制御できます。IP アクセス制御では、あらゆるタイプのトラフィックによる KSX II へのアクセスが制限されるので、NTP サーバ、RADIUS ホスト、DNS ホストなどは、KSX II へのアクセスが許可されている必要があります。

グローバル アクセス制御リスト (ACL) の設定を行い、許可されていない IP アドレスから送信されるパケットにデバイスが応答することのないようにします。IP アクセス制御はグローバルに作用し、KSX II 全体に影響しますが、グループ レベルで KSX II へのアクセスを制御することもできます。グループ レベルの制御の詳細については、「グループ ベースの IP アクセス制御リスト」を参照してください。

重要: KSX II のローカル ポートでは、IP アドレス 127.0.0.1 が使用されます。IP アクセス制御リストを作成する際に、ブロックされる IP アドレス範囲に 127.0.0.1 を含めないでください。そうしなければ、KSX II ローカル ポートにアクセスできなくなります。

▶ IP アクセス制御機能を利用するには

1. [Security] (セキュリティ) の [IP Access Control] (IP アクセス制御) を選択すると、[IP Access Control] (IP アクセス制御) ページが開きます。
2. [Enable IP Access Control] (IP アクセス制御を有効にする) チェックボックスをオンにし、このページの他のフィールドを有効にします。
3. [Default policy] (デフォルト ポリシー) ボックスの一覧で値を選択します。これは、指定した範囲内にない IP アドレスに対して実行されるアクションです。
   - [ACCEPT] (許可): 指定した範囲内にない IP アドレスから KSX II へのアクセスを許可します。
   - [Drop] (拒否): 指定した範囲内にない IP アドレスから KSX II へのアクセスを拒否します。

▶ ルールを一覧の末尾に追加するには

1. [IPv4/Mask or IPv6/Prefix Length] (IPv4/マスクまたは IPv6/プレフィックスの長さ) ボックスに IP アドレスとサブネット マスクを入力します。

   注: IP アドレスは Classless Inter-Domain Routing (CIDR) 方式で入力してください。つまり、先頭の 24 ビットをネットワーク アドレスとして使用します。

2. [Policy] (ポリシー) 列のボックスの一覧でポリシーを選択します。
3. [Append] (追加) をクリックします。そのルールがルール一覧の末尾に追加されます。

ルールを一覧の途中に挿入するには

1. ルール番号を入力します。ルールを一覧の途中に挿入する場合、ルール番号は入力必須です。
2. [IPv4/Mask or IPv6/Prefix Length] (IPv4/マスクまたは IPv6/プレフィックスの長さ) ボックスに IP アドレスとサブネット マスクを入力します。
3. [Policy] (ポリシー) 列のボックスの一覧でポリシーを選択します。
4. [Insert] (挿入) をクリックします。入力したルール番号と同じルール番号のルールが存在する場合、新しいルールはそのルールの上に挿入され、以降のすべてのルールが 1 行下に下がります。

ヒント: ルール番号を使用すると、各ルールを作成する順序を気にせずに済みます。

ルールの内容を置換するには

1. 置換したいルールのルール番号を入力します。
2. [IPv4/Mask or IPv6/Prefix Length] (IPv4/マスクまたは IPv6/プレフィックスの長さ) ボックスに IP アドレスとサブネット マスクを入力します。
3. [Policy] (ポリシー) 列のボックスの一覧でポリシーを選択します。
4. [Replace] (置換) をクリックします。同じルール番号の既存ルールが、新しいルールに置き換わります。

ルールを削除するには

1. 削除したいルールのルール番号を入力します。
2. [Delete] (削除) をクリックします。

3. 削除してよいかどうかを確認するダイアログ ボックスが開きます。[OK] (OK) をクリックします。

SSL 証明書

KSX II では、接続先クライアントとの間で送受信されるトラフィックを暗号化するために Secure Sockets Layer (SSL) が使用されます。

KSX II とクライアントとの接続を確立する際、暗号化された証明書を使用して、KSX II の正当性をクライアントに示す必要があります。

KSX II 上で、証明書署名要求 (CSR) を生成し、証明機関 (CA) によって署名された証明書をインストールすることができます。

CA はまず、CSR 発行元の身元情報を検証します。

続いて、署名された証明書を発行元に返します。有名な CA によって署名されたこの証明書は、証明書発行者の身元を保証する目的で使用されます。

重要: KSX II の日付と時刻が正しく設定されていることを確認します。

自己署名証明書が作成されると、KSX II の日付と時刻を使用して、有効期間が計算されます。KSX II の日付と時刻が正確でない場合、証明書の有効な日付範囲が正しくなくなり、証明書の検証に失敗するおそれがあります。「*日付/時刻の設定* 『*162*p. 』」を参照してください。

注:CSR は、KSX II で生成する必要があります。

注: ファームウェアをアップグレードしても、アクティブな証明書およびCSR は置き換えられません。

▶ SSL 証明書を作成してインストールするには

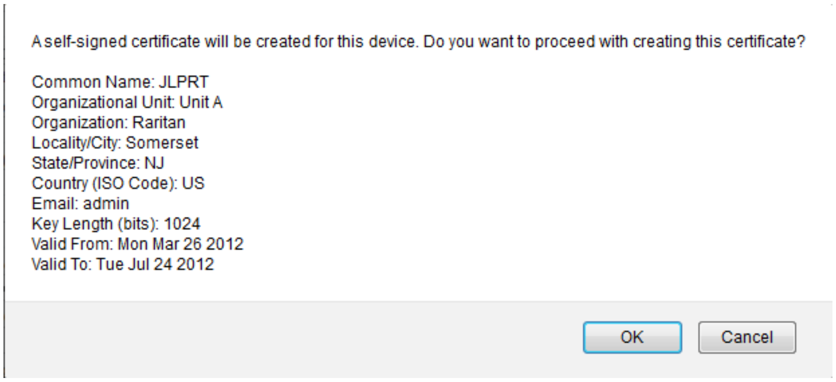
1. [Security] (セキュリティ) メニューの [Certificate] (証明書) を選択します。
2. 次の各フィールドの値を指定します。
   a. [Common name] (共通名) – KSX II をネットワークに追加したときに指定した、KSX II のネットワーク名。通常は完全修飾ドメイン名です。共通名は、Web ブラウザで KSX II にアクセスする際に使用する名前から、プレフィックスである「http://」を除いたものです。ここで指定した名前が実際のネットワーク名と異なる場合は、HTTPS を使用して KSX II にアクセスする際に、ブラウザでセキュリティ警告が表示されます。
   b. [Organizational unit] (組織内部門): KSX II が属する、組織内の部門。
   c. [Organization] (組織): KSX II が属する組織。
   d. [Locality/City] (市区町村): 組織が存在する市区町村。
   e. [State/Province] (都道府県): 組織が存在する都道府県。
   f. [Country (ISO code)] (国 (ISO コード)): 組織が存在する国。2 文字の ISO コードを入力します。たとえば、ドイツの場合は「DE」、米国の場合は「US」と入力します。
   g. [Challenge Password] (チャレンジ パスワード): 一部の CA は、証明書が失効した場合などに証明書の変更を許可するための、チャレンジ パスワードを要求します。CA 証明書の CSR を生成するときに適用されます。
   h. [Confirm Challenge Password] (チャレンジ パスワードの確認入力): 確認のためチャレンジ パスワードを再度入力します。CA 証明書の CSR を生成するときに適用されます。
   i. [Email] (電子メール): KSX II とそのセキュリティを担当する人の電子メール アドレス。
   j. [Key length (bits)] (キー長 (単位: ビット)): 生成されるキーの長さ (単位: ビット)。デフォルト値は [1024] (1024) です。
3. 生成するには、次のいずれかの手順に従います。
   - 自己署名証明書を生成するには、以下の手順に従います。

a. 自己署名証明書を生成する必要がある場合は、[Create a Self-Signed Certificate] (自己署名証明書の作成) チェックボックスをオンにします。このオプションを選択すると、入力内容に基づいて証明書が生成され、KSX II が署名証明機関として機能します。CSR をエクスポートして署名入り証明書の生成に使用する必要はありません。

b. 有効期限の日数を指定します。KSX II の日付と時刻が正しいことを確認し、正しくない場合は、有効な日付を使用して、証明書の有効期限を作成できます。

c. [Create] (作成) をクリックします。

d. 確認ダイアログ ボックスが表示されます。[OK] をクリックして、ダイアログ ボックスを閉じます。

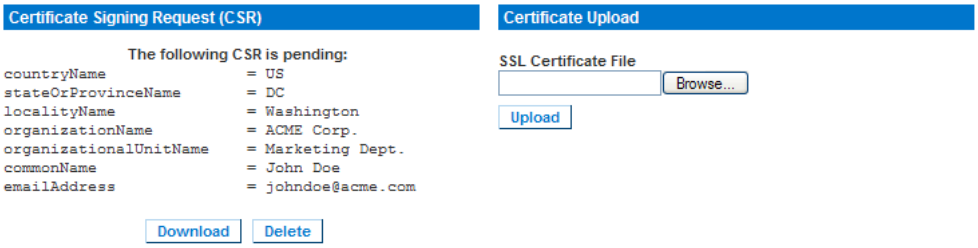


e. KSX II を再起動して自己署名証明書を有効にします。

- CSR を生成して証明書の CA に送信するには、以下の手順に従います。

a. [Create] (作成) をクリックします。

b. 入力したすべての情報を含むメッセージが表示されます。



c. CSR、および CSR 生成時に使用された秘密鍵を含むファイルをダウンロードするには、[Download CSR] (CSR のダウンロード) をクリックします。

d. 証明書を取得するため、保存されている CSR を CA に送信します。CA から新しい証明書が届きます。

注: CSR と秘密鍵ファイルはセットになっているので、そのように扱う必要があります。署名付き証明書が、元の CSR の生成時に使用された秘密鍵と対応していない場合、その証明書は使用できません。このことは、CSR と秘密鍵ファイルのアップロードおよびダウンロードに当てはまります。

- CA から証明書を取得したら、[Upload] (アップロード) をクリックして KSX II にアップロードします。
- KSX II を再起動して証明書を有効にします。

この手順が完了すると、KSX II 専用の証明書が入手されます。この証明書は、KSX II の身元をクライアントに対して示す際に使用されます。

重要: KSX II 上の CSR を破棄した場合、復旧する方法はありません。誤って CSR を削除してしまった場合、前述の 3 つの手順をやり直す必要があります。やり直しを回避するには、ダウンロード機能を利用し、CSR とその秘密鍵のコピーを取得しておきます。

セキュリティ バナー

KSX II ログイン プロセスにセキュリティ バナーを追加できます。この機能により、ユーザは、KSX II にアクセスできるようになる前に、セキュリティ同意書に同意するかどうかの選択を求められます。セキュリティ バナーの内容は、ユーザが自分のログイン資格情報を使用して KSX II にアクセスした後、[Restricted Service Agreement] (制限付きサービス同意書) ダイアログ ボックスに表示されます。

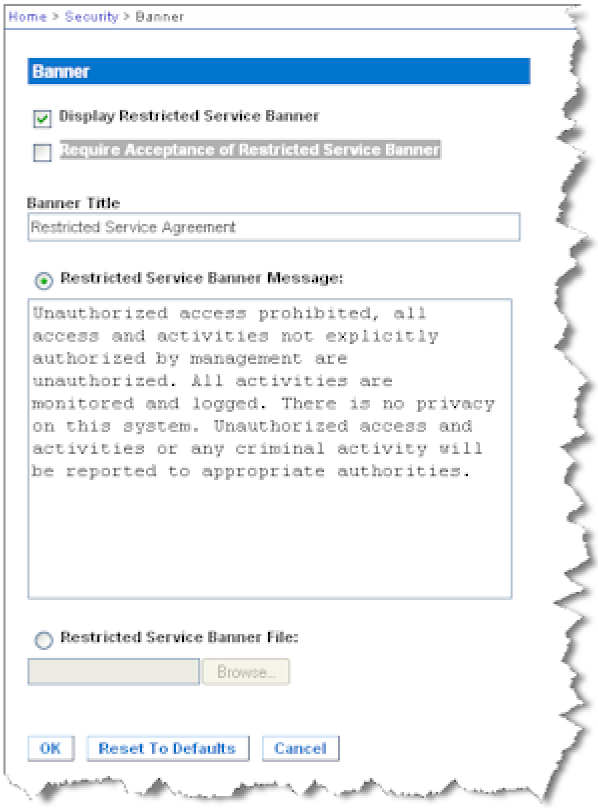
セキュリティ バナーの見出しおよび本文はカスタマイズできます。デフォルトのテキストをそのまま使用することもできます。また、セキュリティ バナーは、ユーザがセキュリティ同意書に同意してからでないと KSX II にアクセスできないように設定することも、単にログイン プロセス終了後に表示することもできます。同意/不同意機能が有効になっている場合、ユーザが選択した内容が監査ログに記録されます。

▶ セキュリティ バナーを設定するには

1. [Security] (セキュリティ) － [Banner] (バナー) をクリックし、[Banner] (バナー) ページを開きます。
2. [Display Restricted Service Banner] (制限付きサービス バナーを表示する) チェック ボックスをオンにし、この機能を有効にします。

3. ユーザがセキュリティ バナーに同意してからでないとログイン プロセスを続行できないようにするには、[Require Acceptance of Restricted Service Banner] (制限付きサービス バナーに対する同意を義務付ける) チェック ボックスをオンにします。ユーザがセキュリティ バナーに同意するには、チェック ボックスをオンにします。この設定を有効にしない場合、ユーザがログインした後にセキュリティ バナーが表示されるだけであり、ユーザがセキュリティ バナーに同意する必要はありません。
4. 必要があれば、バナー タイトルをカスタマイズします。この情報は、バナーの一部としてユーザに対して表示されます。最大 64 文字まで使用できます。
5. [Restricted Services Banner Message] (制限付きサービス バナー メッセージ) ボックス内のテキストをカスタマイズします。入力できるテキストは最大 6,000 文字です。直接入力する方法と、テキスト ファイルからアップロードする方法があります。次のいずれかの手順を実行します。
    a. このボックス内のテキストを手動で編集します。[OK] をクリックします。
    b. .txt ファイル内のテキストをアップロードします。具体的には、[Restricted Services Banner File] (制限付きサービス バナー ファイル) を選択し、[Browse] (参照) をクリックしてファイルを探し、アップロードします。[OK] をクリックします。ファイルがアップロードされると、そのファイル内のテキストが [Restricted Services Banner Message] (制限付きサービス バナー メッセージ) ボックスに表示されます。

注:ローカル ポートからテキスト ファイルをアップロードすることはできません。



Ch 10 保守

この章の内容

メンテナンス機能 (ローカル/リモート コンソール) 227
[Audit Log] (監査ログ) 228
[Device Information] (デバイス情報) 229
バックアップと復元 230
[USB Profile Management] (USB プロファイルの管理) 233
CIM アップグレード 234
[Upgrading Firmware] (ファームウェアのアップグレード) 235
[Upgrade History] (アップグレード履歴) 238
KSX II の再起動 238
CC Unmanage 239

メンテナンス機能 (ローカル/リモート コンソール)

メニュー	目的	ローカル	リモート
[Audit Log] (監査ログ)	日付と時刻順に Dominion KSX II のイベントを表示します。	✓	✓
[Device Information] (デバイス情報)	Dominion KSX II とその CIM に関する情報を表示します。	✓	✓
[Backup/Restore] (バックアップ/リストア)	KSX II の設定をバックアップおよび復元します。		✓
[USB Profile Management] (USB プロファイルの管理)	Raritan のテクニカル サポート部門から提供されたカスタム プロファイル情報をアップロードできます。		✓
[CIM Firmware Upgrade] (CIM ファームウェアのアップグレード)	Dominion KSX II のメモリに保存されているファームウェア バージョンを使用して、CIM をアップグレードします。	✓	✓
[Firmware Upgrade] (ファームウェアのアップグレード)	Dominion KSX II ファームウェアをアップグレードします。		✓

メニュー	目的	ローカル	リモート
[Factory Reset] (出荷時設定にリセット)	ファクトリ リセットを行います。	✓	
[Upgrade History] (アップグレード履歴)	最後に行ったアップグレードに関する情報を表示します。	✓	✓
[Reboot] (再起動)	KSX II を再起動します。	✓	✓

[Audit Log] (監査ログ)

KSX II のシステム イベントに関するログが作成されます。監査ログは最大で約 2K 分のデータを保持でき、これを超えると最も古いエントリから上書きされます。監査ログのデータが失われないようにするには、syslog サーバまたは SNMP マネージャにデータをエクスポートします。syslog サーバまたは SNMP マネージャは、[Device Settings] (デバイス設定) の [Event Management] (イベント管理) ページから設定します。

▶ KSX II の監査ログを表示するには

1. [Maintenance] (保守) メニューの [Audit Log] (監査ログ) をクリックします。[Audit Log] (監査ログ) ページが開きます。

   [Audit Log] (監査ログ) ページでは、日時順にイベントが表示されます (最も新しいイベントが先頭に表示されます)。監査ログに含まれる情報は次のとおりです。

   - [Date] (日時): イベントが発生した日時 (24 時間形式)。
   - [Event] (イベント): [Event Management] (イベント管理) ページに一覧表示されるイベント名。
   - [Description] (説明): イベントの詳細な説明。

▶ 監査ログを保存するには

注: 監査ログの保存は KSX II リモート コンソールでのみ実行できます。KSX II ローカル コンソールでは実行できません。

1. [Save to File] (ファイルに保存) をクリックします。[Save File] (ファイルに保存) ダイアログ ボックスが開きます。
2. ファイル名と保存先フォルダを選択し、[Save] (保存) をクリックします。監査ログが、クライアント コンピュータ上の指定した保存先フォルダに指定した名前で保存されます。

監査ログのページ間を移動するには

- [Older] (古いログへ) リンクおよび [Newer] (新しいログへ) リンクを使用します。

[Device Information] (デバイス情報)

[Device Information] (デバイス情報) ページには、使用している KSX II デバイスとコンピュータ インタフェース モジュール (CIM) に関する詳細情報が表示されます。これらの情報は、Raritan のテクニカル サポート部門に問い合わせをする際に役立ちます。

使用している Dominion KSX II と CIM に関する情報を表示するには、以下の手順に従います。

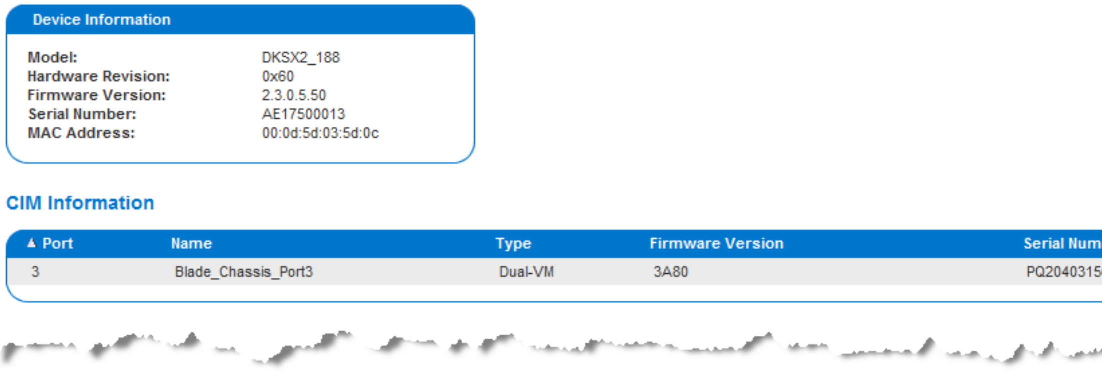
- [Maintenance] (保守) メニューの [Device Information] (デバイス情報) をクリックします。[Device Information] (デバイス情報) ページが開きます。

使用している KSX II に関する以下の情報が提供されます。

- [Model] (モデル)
- [Hardware Revision] (ハードウェア リビジョン)
- [Firmware Version] (ファームウェア バージョン)
- [Serial Number] (シリアル番号)
- [MAC Address] (MAC アドレス)

CIM に関して表示される情報は次のとおりです。

- [Port] (ポート) (番号)
- [Name] (名前)
- [Type] (タイプ) (CIM、電源タップ、および VM)
- [Firmware Version] (ファームウェア バージョン)
- [Serial Number] (シリアル番号)



バックアップと復元

[Backup/Restore] (バックアップ/復元) ページでは、KSX II の設定情報をバックアップおよび復元できます。

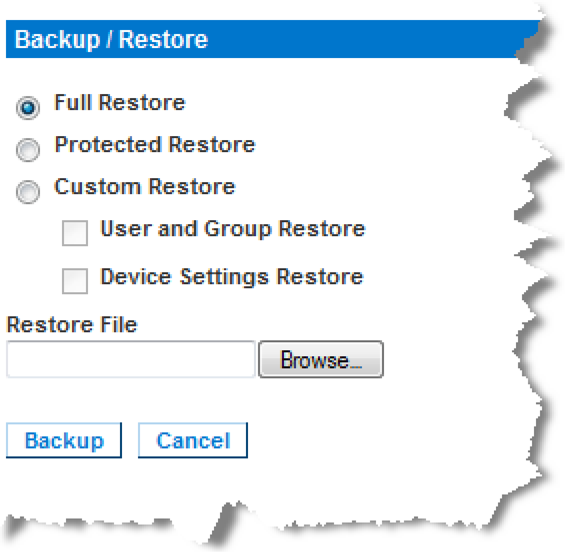
バックアップ/復元機能には、業務継続性を確保するというメリットに加え、時間節約効果もあります。

たとえば、使用中の KSX II のユーザ設定情報をバックアップして別の KSX II に復元することにより、その復元先 KSX II をすぐに使用できるようになります。

また、1 台の KSX II をセットアップし、その設定情報を複数台の KSX II にコピーすることもできます。

[Backup/Restore] (バックアップ/復元) ページを開くには

- [Maintenance] (保守) メニューの [Backup/Restore] (バックアップ/復元) をクリックします。[Backup/Restore] (バックアップ/復元) ページが開きます。



注:バックアップ処理では、常にシステム全体がバックアップされます。復元処理では、全体を復元するか一部を復元するかをユーザが選択できます。

Internet Explorer 7 以降を使用している場合、KSX II をバックアップするには、以下の手順に従います。

1. [Backup] (バックアップ) をクリックします。[Open] (開く) ボタンを含む [File Download] (ファイルのダウンロード) ダイアログ ボックスが開きます。[Open] (開く) をクリックしないでください。

IE 7 (以降) では、ファイルを開くデフォルトのアプリケーションとして IE が使用されるため、ファイルを開くか、または保存するように求められます。これを回避するには、ファイルを開くために使用されるデフォルトのアプリケーションをワードパッド® に変更する必要があります。

2. このためには、以下の手順に従います。
   a. バックアップ ファイルを保存します。バックアップ ファイルが、クライアント コンピュータ上の指定した保存先フォルダに指定した名前で保存されます。
   b. 保存されたら、ファイルを探して右クリックします。[プロパティ] を選択します。
   c. [全般] タブで [変更] をクリックし、[WordPad] を選択します。

▶ KSX II を復元するには

警告: 使用している KSX II を旧バージョンに復元する場合、注意が必要です。バックアップ時点で設定されていたユーザ名とパスワードが復元されます。つまり、バックアップ時点での管理者のユーザ名とパスワードを覚えていない場合、KSX II からロックアウトされます。

また、バックアップ時点で現在と異なる IP アドレスを使用していた場合、その IP アドレスも同様に復元されます。IP アドレスの割り当てに DHCP を使用している場合、ローカル ポートにアクセスして復元後の IP アドレスを調べる必要があります。

1. 実行する復元処理のタイプを選択します。
   - [Full Restore] (完全復元): システム全体を復元します。この復元タイプの主な用途は、一般的なバックアップ/復元処理です。
   - [Protected Restore] (部分復元): デバイス固有情報 (例: IP アドレス、名前) 以外のすべての情報が復元されます。この復元タイプの用途としては、1 台の KSX II をセットアップし、その設定情報を複数台の KSX II にコピーするケースなどが考えられます。
   - [Custom Restore] (カスタム復元): この復元タイプを選択した場合、[User and Group Restore] (ユーザとグループの復元) チェック ボックスと [Device Settings Restore] (デバイス設定の復元) チェック ボックスのいずれか一方または両方をオンにすることができます。

- [User and Group Restore] (ユーザとグループの復元): このチェック ボックスをオンにした場合、ユーザ情報とグループ情報だけが復元されます。証明書および秘密鍵ファイルは*復元されません*。別の KSX II 上でユーザ情報をセットアップする際に便利です。
- [Device Settings Restore] (デバイス設定の復元): このチェック ボックスをオンにした場合、デバイス設定情報 (例: 関連電源、USB プロファイル、ブレード シャーシ関連の設定パラメータ、ポート グループの割り当て) だけが復元されます。デバイス情報をコピーする際に便利です。

2. [Browse] (参照) をクリックします。[Choose file] (ファイルを選択) ダイアログ ボックスが開きます。
3. 適切なバックアップ ファイルを探して選択し、[Open] (開く) をクリックします。選択したファイルが [Restore File] (復元ファイル) ボックスに表示されます。
4. [Restore] (復元) をクリックします。選択した復元タイプに基づいて、設定情報が復元されます。

[USB Profile Management] (USB プロファイルの管理)

[USB Profile Management] (USB プロファイル管理) ページでは、Raritan のテクニカル サポート部門から提供されたカスタム プロファイル情報をアップロードできます。これらのプロファイルは、標準プロファイルがターゲット サーバ構成のニーズに対応していない場合にそのニーズに対応できるよう、設計されています。Raritan のテクニカル サポートは、カスタム プロファイルを提供し、ターゲット サーバ固有のニーズに対する解決策をお客様と一緒に探します。

[USB Profile Management] (USB プロファイル管理) ページを開くには

- [Maintenance] (保守) メニューの [USB Profile Management] (USB プロファイル管理) をクリックします。[USB Profile Management] (USB プロファイル管理) ページが開きます。

カスタム プロファイル情報を KSX II にアップロードするには

1. [Browse] (参照) をクリックします。[Choose file] (ファイルを選択) ダイアログ ボックスが開きます。
2. 適切なカスタム プロファイル ファイルを探して選択し、[Open] (開く) をクリックします。選択したファイルが [USB Profile File] (USB プロファイル ファイル) ボックスに表示されます。
3. [Upload] (アップロード) をクリックします。カスタム プロファイル情報がアップロードされ、プロファイル一覧に表示されます。

注:アップロード処理中にエラーまたは警告が表示された場合 (例: 既存のカスタム プロファイルが上書きされる場合)、アップロード処理を続行するには [Upload] (アップロード)、アップロード処理をキャンセルするには [Cancel] (キャンセル) をクリックします。

▶ **カスタム プロファイル情報を KSX II から削除するには**

1. 削除するカスタム プロファイルのチェック ボックスをオンにします。
2. [Delete] (削除) をクリックします。カスタム プロファイル情報が削除され、プロファイル一覧に表示されなくなります。

アクティブになっているカスタム プロファイルでも削除できます。ただしその場合、確立されていた仮想メディア セッションがすべて終了します。

プロファイル名の競合を処理する

ファームウェアをアップグレードしたとき、カスタム USB プロファイルと標準 USB プロファイルの名前が競合することがあります。たとえば、あるカスタム プロファイルを作成して標準プロファイル リストに組み込んでおり、ファームウェアのアップグレード時に同名の USB プロファイルがダウンロードされた場合などです。

この場合、既存のカスタム プロファイルの名前に old_ というプレフィックスが付加されます。たとえば、GenericUSBProfile5 という名前のカスタム プロファイルが存在しており、かつ、ファームウェアのアップグレード時に同名のプロファイルがダウンロードされた場合、既存のカスタム プロファイルの名前が old_GenericUSBProfile5 に変更されます。

必要に応じて、既存のプロファイルを削除できます。詳細については、「*USB プロファイルの管理* 『*233*p. の"*[USB Profile Management] (USB プロファイルの管理)*"参照 』」を参照してください。

CIM アップグレード

この項で説明する手順に従って、KSX II のメモリに格納されているファームウェア バージョンを基に CIM をアップグレードします。一般に、[Firmware Upgrade] (ファームウェアのアップグレード) ページを使用してデバイスのファームウェアをアップグレードする場合、すべての CIM がアップグレードされます。

▶ **KSX II のメモリを使用して CIM をアップグレードするには**

1. [Maintenance] (保守) メニューの [CIM Firmware Upgrade] (CIM ファームウェアのアップグレード) をクリックします。[CIM Upgrade from] (CIM のアップグレード) ページが開きます。

[Port] (ポート)、[Name] (名前)、[Type] (タイプ)、[Current CIM Version] (現在の CIM バージョン)、[Upgrade CIM Version] (アップグレード先の CIM バージョン) の各列に情報が表示されるので、各 CIM を簡単に識別できます。

2. アップグレードしたい各 CIM の [Selected] (選択) チェック ボックスをオンにします。
3. [Upgrade] (アップグレード) をクリックします。アップグレードしてもよいかどうかを確認するダイアログ ボックスが開きます。
4. [OK] をクリックしてアップグレード処理を続行します。アップグレード処理中は、進行状況バーが表示されます。アップグレード処理には、CIM ごとに最長で約 2 分かかります。

[Upgrading Firmware] (ファームウェアのアップグレード)

[Firmware Upgrade] (ファームウェアのアップグレード) ページを使用して、KSX II および接続するすべての CIM のファームウェアをアップグレードします。このページは、KSX II リモート コンソールでのみ使用できます。

重要: アップグレード処理中に、KSX II の電源を切断したり CIM を取り外したりしないでください。KSX II または CIM が損傷するおそれがあります。

▶ **KSX II をアップグレードするには、以下の手順に従います。**

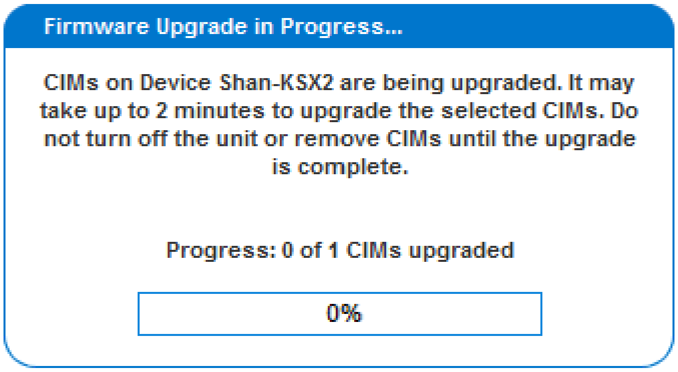
1. 該当する Raritan ファームウェアの配布ファイル (*.RFP 形式) を指定します。このファイルは、Raritan 社 のファームウェア アップグレード Web ページから入手できます。http://www.raritan.com/support/firmwareupgrades にアクセスして、ファイルをダウンロードしてください。
2. そのファイルを解凍します。アップグレードを実行する前に、解凍したファイルに記載されている指示をすべてお読みください。
3. アップグレードを実行する前に、そのファームウェア配布ファイルをローカル PC にコピーしておいてください。また、そのファームウェア配布ファイルをネットワーク ドライブからロードしないでください。

4. [Maintenance] (保守) メニューの [Firmware Upgrade] (ファームウェアのアップグレード) をクリックします。[Firmware Upgrade] (ファームウェアのアップグレード) ページが開きます。

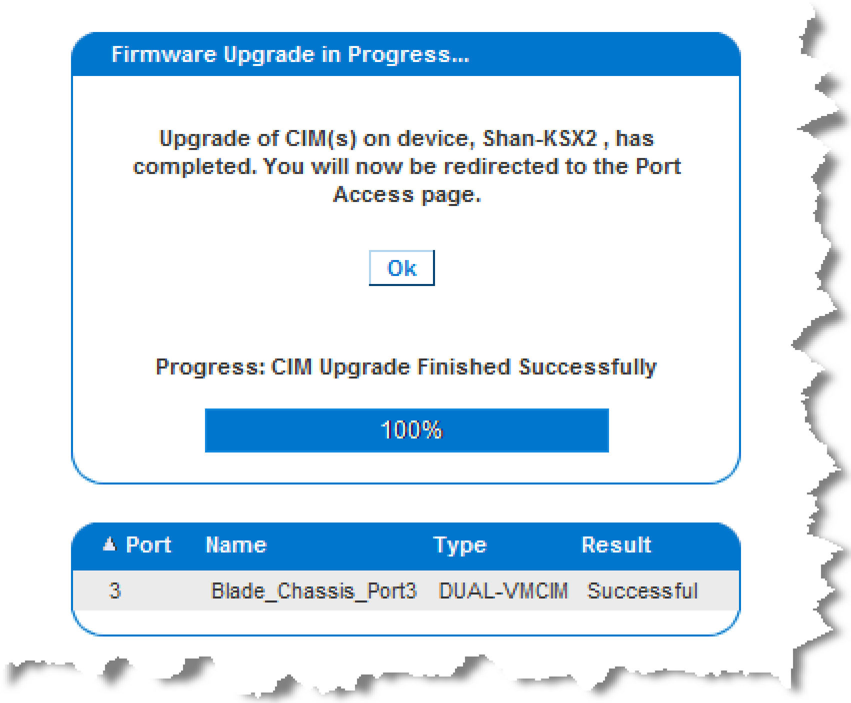
5. [Browse] (参照) をクリックし、ファームウェア配布ファイルを解凍したフォルダに移動します。
6. 使用している CIM のバージョン情報を表示したい場合、[Review CIM Version Information?] (CIM のバージョン情報を確認する) チェックボックスをオンにします。
7. [Firmware Upgrade] (ファームウェアのアップグレード) ページの [Upload] (アップロード) をクリックします。アップグレードとバージョン番号に関する情報が表示されます。CIM 情報を表示するよう指定した場合は、その情報も表示されます。

注: この時点で接続していたユーザはログオフされ、新たにログオンしようとしたユーザはブロックされます。

8. [Upgrade] (アップグレード) をクリックし、アップグレード処理が完了するまで待機します。アップグレード処理中は、ステータス情報および進行状況バーが表示されます。アップグレードが完了すると、デバイスは再起動します (再起動を知らせるビープ音が 1 回鳴ります)。



9. 指示に従ってブラウザを終了し、約 5 分待ってから再度 KSX II にログオンします。

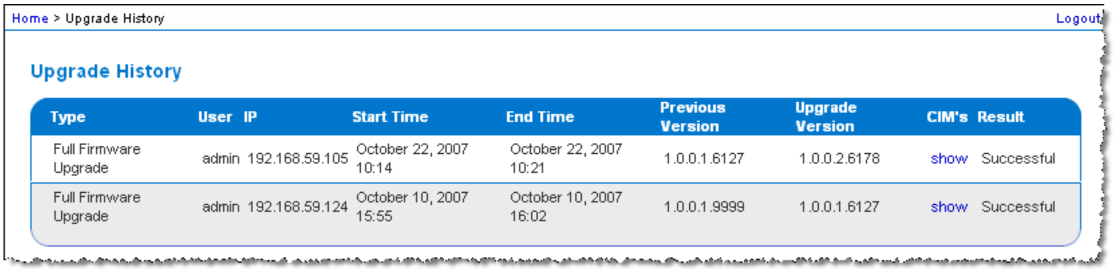


[Upgrade History] (アップグレード履歴)

KSX II および接続されている CIM に対して実行されたアップグレード処理に関する情報を表示できます。

▶ アップグレード履歴を表示するには

- [Maintenance] (保守) メニューの [Upgrade History] (アップグレード履歴) をクリックします。[Upgrade History] (アップグレード履歴) ページが開きます。



Type	User	IP	Start Time	End Time	Previous Version	Upgrade Version	CIM's	Result
Full Firmware Upgrade	admin	192.168.59.105	October 22, 2007 10:14	October 22, 2007 10:21	1.0.0.1.6127	1.0.0.2.6178	show	Successful
Full Firmware Upgrade	admin	192.168.59.124	October 10, 2007 15:55	October 10, 2007 16:02	1.0.0.1.9999	1.0.0.1.6127	show	Successful

実行された KSX II アップグレード処理に関する情報、アップグレード処理の最終ステータス、アップグレード処理の開始日時と終了日時、および、アップグレード前と現在のファームウェア バージョンが表示されます。CIM に関する情報を表示するには、[CIM's] (CIM) 列の [show] (表示) リンクをクリックします。表示される CIM 情報は次のとおりです。

- [Port] (ポート): CIM が接続されているポート。
- [Name] (名前) – CIM の名前。
- [Type] (タイプ): CIM のタイプ。
- [Previous Version] (アップグレード前のバージョン): アップグレード前の CIM バージョン。
- [Upgrade Version] (アップグレード後のバージョン): 現在の CIM バージョン。
- [Result] (結果): アップグレード処理の結果 (成功または失敗)。
-

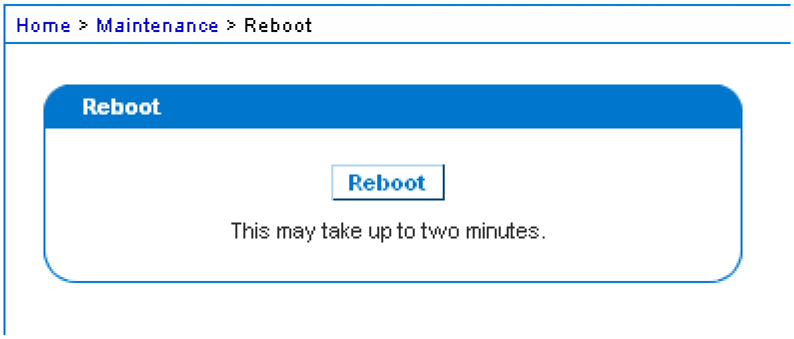
KSX II の再起動

[Reboot] (再起動) ページでは、KSX II を安全に再起動できます。再起動する場合、このページから行うことを推奨します。

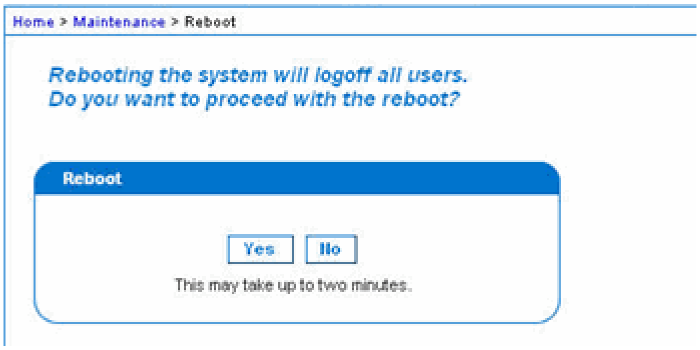
重要: すべての KVM 接続およびシリアル接続が切断され、また、すべてのユーザがログオフされます。

▶ KSX II を再起動するには

1. [Maintenance] (保守) メニューの [Reboot] (再起動) をクリックします。[Reboot] (再起動) ページが開きます。

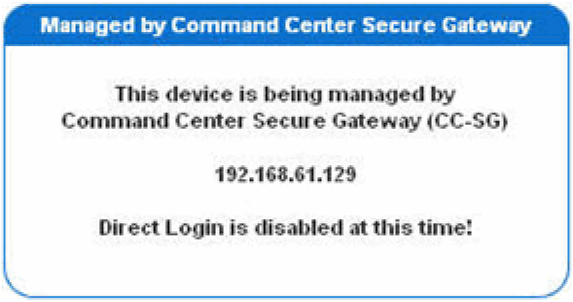


2. [Reboot] (再起動) をクリックします。再起動してもよいかどうかを確認するダイアログ ボックスが開きます。[Yes] (はい) をクリックし、再起動処理を続行します。



CC Unmanage

KSX II デバイスが CommandCenter Secure Gateway の管理下にあるとき、KSX II リモート コンソールを使用してデバイスに直接アクセスを試みると、次のメッセージが表示されます (有効なユーザ名とパスワードの入力後)。



CC-SG 管理の終了

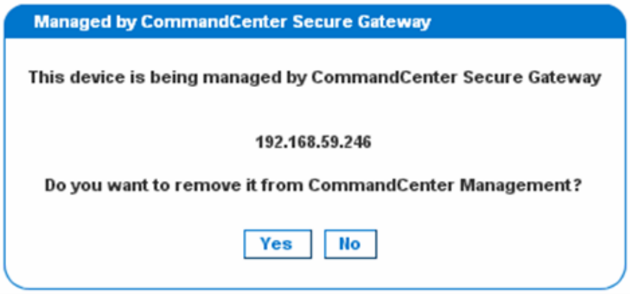
KSX II が CommandCenter Secure Gateway (CC-SG) の管理下にあるのに、KSX II に直接アクセスしようとすると、KSX II が CC-SG の管理下にあることを示すメッセージが表示されます。

KSX II が CC-SG の管理下にあるが、指定タイムアウト間隔 (通常は 10 分) が経過した後に CC-SG と KSX II の間の接続が切断された場合、KSX II コンソールから CC-SG 管理セッションを終了できます。

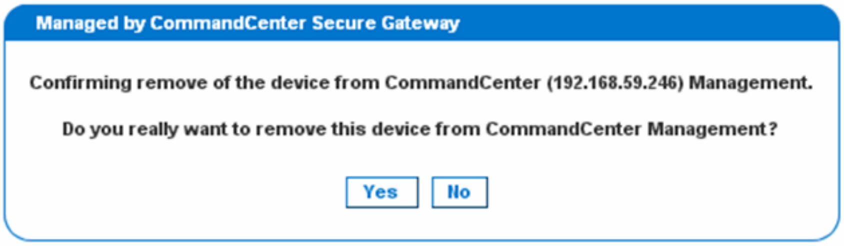
注:KSX II を CC-SG の管理対象から除外するには、適切な権限が必要です。また、KSX II が現在 CC-SG の管理下にない場合、[Maintenance] (保守) メニューの [Stop CC-SG Management] (CC-SG の管理対象から除外する) コマンドは無効になります。

▶ KSX II を CC-SG の管理対象から除外するには、以下の手順に従います。

1. [Maintenance] (保守) メニューの [Stop CC-SG Management] (CC-SG の管理対象から除外する) をクリックします。"KSX II が CC-SG の管理下にある" という内容のメッセージが表示されます。また、KSX II を CC-SG の管理対象から除外するためのボタンも表示されます。



2. [Yes] (はい) をクリックし、KSX II を CC-SG の管理対象から除外する処理を開始します。KSX II を CC-SG の管理対象から除外してもよいかどうかを確認するためのメッセージが表示されます。



3. [Yes] (はい) をクリックし、KSX II を CC-SG の管理対象から除外します。KSX II が CC-SG の管理対象から除外されると、処理完了メッセージが表示されます。

Ch 11 診断

[Diagnostics] (診断) ページはトラブルシューティングの目的で使用されるページであり、主に KSX II デバイスの管理者を対象としています。すべての [Diagnostics] (診断) ページで ([Device Diagnostics] (デバイス診断) を除く)、標準的なネットワーク コマンドが実行されます。表示される情報は、それらのコマンドの出力結果です。[Diagnostics] (診断) メニュー オプションは、ネットワーク設定のデバッグと変更に役立ちます。

[Device Diagnostics] (デバイス診断) は、Raritan テクニカル サポートの指示に従って使用するオプションです。

この章の内容

[Network Interface] (ネットワーク インタフェース) ページ............... 242
[Network Statistics] (ネットワーク統計) ページ................................ 243
[Ping Host] (ホストに ping する) ページ... 245
[Trace Route to Host (ホストへのルートの追跡)] ページ 245
[KSX II Diagnostics] (KSX II 診断) ページ 246

[Network Interface] (ネットワーク インタフェース) ページ

KSX II では、ネットワーク インタフェースのステータス情報を確認できます。

▶ ネットワーク インタフェースに関する情報を表示するには

- [Diagnostics] (診断) メニューの [Network Interface] (ネットワーク インタフェース) をクリックします。[Network Interface] (ネットワーク インタフェース) ページが開きます。

表示される情報は次のとおりです。

- Ethernet インタフェースが稼動しているかどうか。
- ゲートウェイから ping できるかどうか。
- 現在アクティブな LAN ポート。

▶ これらの情報を更新するには

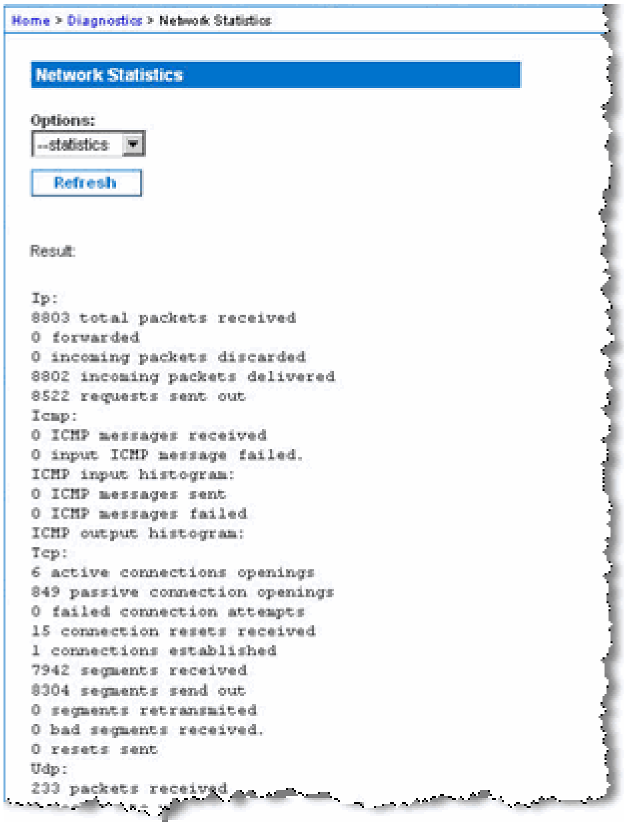
- [Refresh] (更新) をクリックします。

[Network Statistics] (ネットワーク統計) ページ

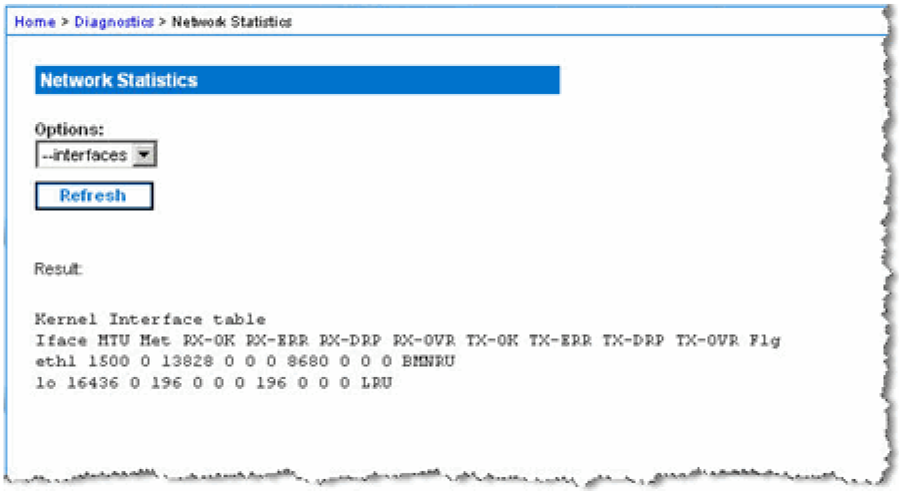
KSX II では、ネットワーク インタフェースに関する統計情報を表示できます。

▶ ネットワーク インタフェースに関する統計情報を表示するには

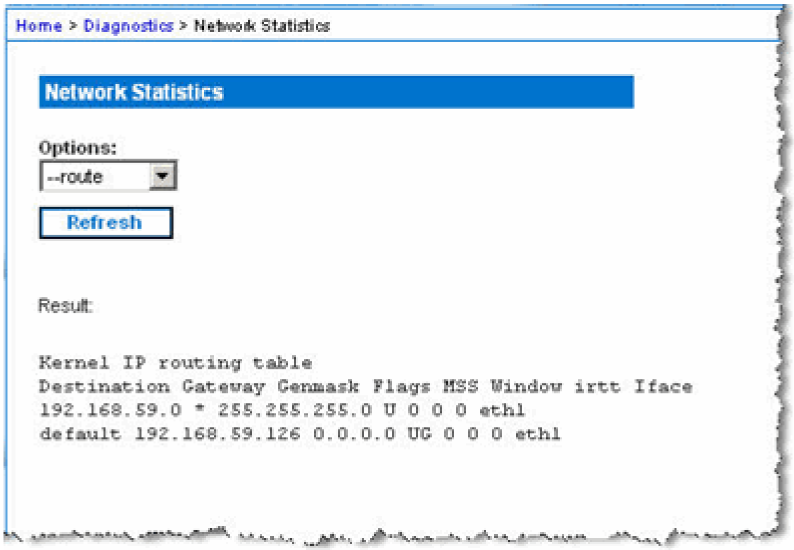
1. [Diagnostics] (診断) メニューの [Network Statistics] (ネットワーク統計) をクリックします。[Network Statistics] (ネットワーク統計) ページが開きます。
2. [Options] (オプション) ボックスの一覧で値を選択します。
   - [Statistics] (統計): 次に示すような情報が表示されます。



- [Interfaces] (インタフェース): 次に示すような情報が表示されます。



- [Route] (経路): 次に示すような情報が表示されます。



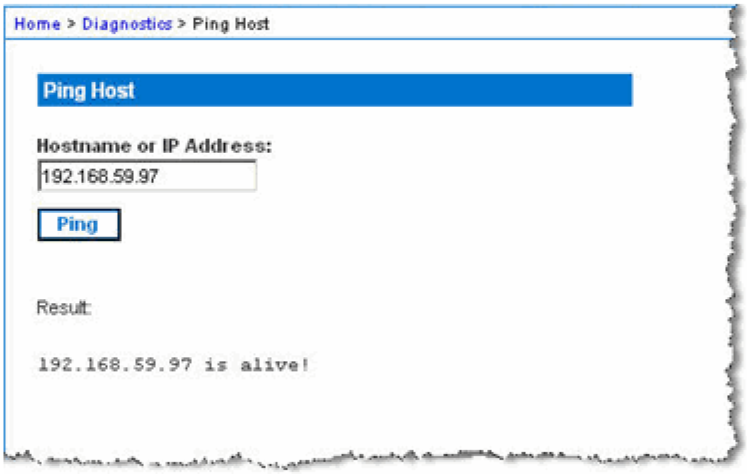
3. [Refresh] (更新) をクリックします。[Options] (オプション) ボックスの一覧で選択した値に応じた情報が、[Result] (結果) フィールドに表示されます。

[Ping Host] (ホストに ping する) ページ

ping は、特定のホストまたは IP アドレスが IP ネットワーク上で接続可能であるかどうかをテストするためのネットワーク コマンドです。[Ping Host] (ホストに ping する) ページでは、ターゲット サーバまたは別の KSX II がアクセス可能であるかどうかを調べることができます。

▶ **ホストに ping するには、以下の手順に従います。**

1. [Diagnostics] (診断) メニューの [Ping Host] (ホストに ping する) をクリックします。[Ping Host] (ホストへの Ping) ページが開きます。



2. [Hostname or IP Address] (ホスト名または IP アドレス) フィールドにホスト名または IP アドレスを入力します。
3. [Ping] をクリックします。ping の実行結果が [Result] (結果) フィールドに表示されます。

[Trace Route to Host (ホストへのルートの追跡)] ページ

trace route (ルートの追跡) は、指定したホスト名または IP アドレスへのルートを調べるためのネットワーク ツールです。

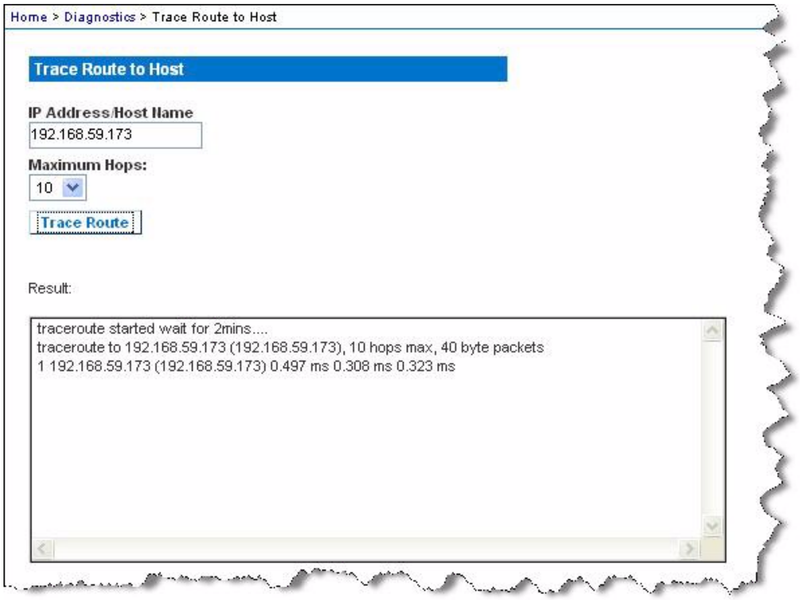
▶ **ホストへのルートを追跡するには、次の手順に従います。**

1. [Diagnostics (診断)] > [Trace Route to Host (ホストへのルートの追跡)] を選択します。[Trace Route to Host (ホストへのルートの追跡)] ページが表示されます。
2. [IP Address/Host Name (IP アドレス/ホスト名)] フィールドに IP アドレスまたはホスト名を入力します。

   注: ホスト名は最大 232 文字です。

3. ドロップダウン リストから最大ホップ数を選択します (5 刻みで 5 ～ 50)。

4. [Trace Route (ルートの追跡)] をクリックします。指定したホスト名または IP アドレスに対して、trace route コマンドが、指定した最大ホップ数以内で実行されます。trace route の実行結果が [Result (結果)] フィールドに表示されます。



[KSX II Diagnostics] (KSX II 診断) ページ

注: これは、Raritan フィールド エンジニアが使用するためのページです。Raritan のテクニカル サポート部門から指示された場合に限り、ユーザも使用できます。

[Device Diagnostics] (デバイス診断) ページでは、診断情報を KSX II からクライアント コンピュータにダウンロードできます。このページでは、次の 2 種類の処理を行うことができます。

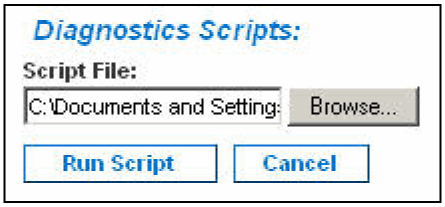
操作	説明
診断スクリプト	重大なエラーのデバッグ セッション中に Raritan テクニカル サポートの提供する特別なスクリプトを実行します。このスクリプトは、KSX II にアップロードされ、実行されます。このスクリプトの実行が完了した後、[Save to File] (ファイルに保存) をクリックして診断メッセージをダウンロードすることができます。
デバイス診断ログ	診断メッセージのスナップショットを KSX II ユニットからクライアントにダウンロード

操作	説明
	します。この暗号化されたファイルは、その後 Raritan テクニカル サポートに送信されます。このファイルは、Raritan でのみ解析できます。

注: このページを開くことができるのは、管理者権限を持つユーザだけです。

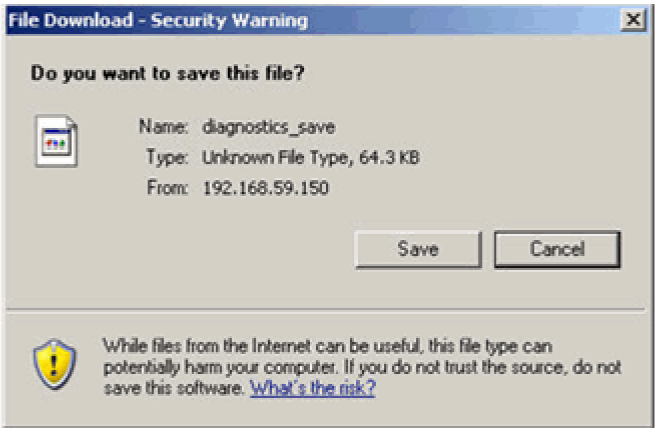
KSX II のシステム診断を実行するには、以下の手順に従います。

1. [Diagnostics] (診断) の [Device Diagnostics] (デバイス診断) を選択します。[Device Diagnostics] (デバイス診断) ページが開きます。
2. Raritan のテクニカル サポート部門から電子メールで受け取った診断スクリプト ファイルを実行するため、次の手順を実行します。
    a. Raritan から提供されている診断スクリプト ファイルを入手します。圧縮されている場合は解凍します。
    b. [Browse] (参照) をクリックします。[Choose file] (ファイルを選択) ダイアログ ボックスが開きます。
    c. その診断ファイルに移動し、選択します。
    d. [Open] (開く) をクリックします。[Script File] (スクリプト ファイル) フィールドにファイルが表示されます。



    e. [Run Script] (スクリプトを実行) をクリックします。
    f. 手順 4 に従って、Raritan テクニカル サポートにこのファイルを送信します。
3. 診断ファイルを作成して Raritan のテクニカル サポート部門に送信するため、次の手順を実行します。

a. [Save to File] (ファイルに保存) をクリックします。[File Download] (ファイルのダウンロード) ダイアログ ボックスが開きます。



b. [Save] (保存) をクリックします。[Save As] (名前を付けて保存) ダイアログ ボックスが開きます。

c. 保存先フォルダに移動し、[Save] (保存) をクリックします。

4. Raritan のテクニカル サポート部門の指示に従って、このファイルを電子メールで送信します。

Ch 12 コマンド ライン インタフェース (CLI)

この章の内容

概要 250
CLI を使用しての KSX II へのアクセス 251
KSX II への SSH 接続 251
KSX II への Telnet 接続 252
KSX II へのローカル シリアル ポート接続 253
ログオン 253
CLI の画面操作 255
CLI を使用した初期設定 257
CLI プロンプト 258
CLI コマンド 258
ターゲット接続と CLI 259
KSX II コンソール サーバ設定用コマンドを使用する 260
ネットワークを設定する 260

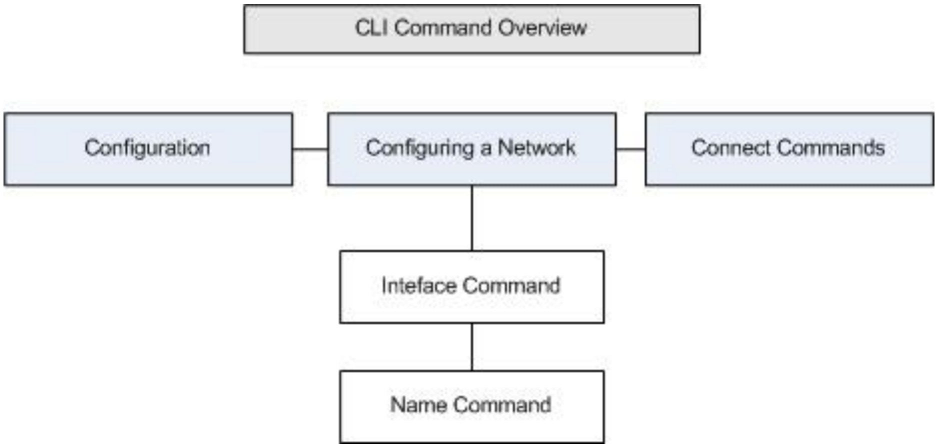
概要

KSX II Serial Console は、以下のようなすべてのシリアル デバイスをすべてサポートしています。

- Emergency Management Services (EMS) による Special Administration Console (SAC)、またはサーバ BIOS の BIOS リダイレクトによる SAC を使用している Windows Server 2003® などのサーバ。
- ルータ
- レイヤ 2 スイッチ
- ファイアウォール
- ラック PDU (電源タップ)
- その他のユーザ装置

KSX II により、管理者やユーザは、複数のシリアル デバイスにアクセスしたり、これらのデバイスを制御および管理できます。コマンド ライン インタフェース (CLI) を使用し、KSX II を設定したり、ターゲット デバイスに接続したりできます。RS-232 インタフェースは、1200 bps ～ 115.2 kbps の標準的なレートで動作します。デフォルトの設定は 9600 bps、8 データ ビット、パリティ ビットなし、1 ストップ ビット、およびフロー制御なしです。

次の図に CLI コマンドの概要を示します。コマンドの一覧については、「*CLI コマンド* 『*258*p. 』」を参照してください。この一覧には、各コマンドの説明、および、各コマンドの記述例が書かれている項へのリンクがあります。



top、history、log off、quit、show、help の各コマンドは、この図のどの CLI レベルからでも使用できます。

CLI を使用しての KSX II へのアクセス

次の方法のいずれかを使用して、KSX II にアクセスします。

- IP 接続を介した Telnet
- IP 接続を介した SSH (Secure Shell)
- RS-232 シリアル インタフェースを介したローカル ポート

複数の SSH/Telnet クライアントを使用可能で、次の場所から取得できます。

- Putty – *http://www.chiark.greenend.org.uk/~sgtatham/putty/ http://www.chiark.greenend.org.uk/~sgtatham/putty/*参照
- ssh.com の SSH クライアント – *www.ssh.com http://www.ssh.com* 参照
- Applet SSH Client – *www.netspace.org/ssh http://www.netspace.org/ssh* 参照
- OpenSSH Client – *www.openssh.org http://www.openssh.org* 参照

KSX II への SSH 接続

SSHv2 をサポートする Secure Shell (SSH) クライアントを使用して、KSX II に接続します。[Devices Services] (デバイス サービス) ページで SSH 接続を有効にしておく必要があります。

注: セキュリティ上の理由により、SSHv1 接続は KSX II でサポートされていません。

Windows PC からの SSH アクセス

Windows® PC から SSH セッションを開くには

1. SSH クライアント ソフトウェアを起動します。
2. KSX II サーバの IP アドレスを入力します (例: 「192.168.0.192」)。
3. SSH を選択します。SSH では、デフォルトの設定ポート 22 が使用されます。
4. [Open] (開く) をクリックします。
5. `login as:` (ログイン) プロンプトが表示されます。

UNIX/Linux ワークステーションからの SSH アクセス

▶ **UNIX®/Linux® ワークステーションから SSH セッションを開き、ユーザ admin としてログオンするため、次のコマンドを入力します。**

```
ssh -l admin 192.168.30.222
```

パスワードの入力を求めるプロンプトが表示されます。

KSX II への Telnet 接続

Telnet はセキュリティが低く、ユーザ名、パスワード、およびすべてのトラフィックが平文で送信されます。Telnet 接続はデフォルトで無効になっています。

Telnet 接続を有効にする

Telnet を使用して KSX II に接続したい場合、まず、CLI またはブラウザを使用して KSX II に接続します。

▶ **Telnet 接続を有効にするには**

1. [Device Settings] (デバイス設定) を選択し、[Enable TELNET Access] (TELNET アクセスを有効にする) チェックボックスを選択します。
2. Telnet ポートを入力します。
3. [OK] をクリックします。

Telnet 接続が有効になったら、Telnet を使用して KSX II に接続し、他のパラメータ値を設定することができます。

Windows PC から Telnet で接続する

▶ **Windows® PC から Telnet セッションを開くには**

1. [スタート] メニューの [ファイル名を指定して実行] をクリックします。
2. [名前] ボックスに「telnet」と入力します。
3. [OK] (OK) をクリックします。Telnet ウィンドウが開きます。
4. プロンプトで `Microsoft Telnet> open <IP address>` と入力します。<IP address> は KSX II の IP アドレスです。
5. Enter キーを押します。次のメッセージが表示されます。「`Connecting To <IP address>...`」(<IP アドレス>に接続しています...) `login as` (ログイン) プロンプトが表示されます。

KSX II へのローカル シリアル ポート接続

KSX II のローカル シリアル ポートは、コンピュータ システム、ターミナルまたは他の適切なシリアル デバイスの COM ポートに、両端が DB-9F の Null モデム ケーブルを使用して接続する必要があります。

KSX II のターミナル ポートで RJ45 ジャックを使用する場合、クライアント マシンでは ASCSDB9F コネクタの付いた特別なケーブル (CRLVR) が使用されます。CRLVR は、ローカル ポートに対して RJ45 対 RJ45 の接続が確立された場合にも使用されます。つまり、KSX II デバイスのローカル ポートを、他の KSX II へのシリアル ターゲットとして接続する場合です。

ポート設定

ポート設定（シリアル通信パラメータ）を以下のように設定してください。

- データ ビット = 8
- パリティ = なし
- ストップ ビット =1
- フロー制御 = なし
- Bits per second (ビット/秒) = 9600

ログオン

▶ **ログインするには、次のようにユーザ名 admin を入力します。**

1. admin としてログインします。
2. パスワードの入力を求めるプロンプトが表示されます。デフォルト パスワード（「*raritan*」）を入力します。

   歓迎メッセージが表示されます。これで、管理者としてログオンしたことになります。

次項「*CLI の画面操作* 『*255*p. 』」の内容を確認した後、初期設定処理を実行します。

```
Welcome!
192.168.59.202 login:admin
Passwd:
--------------------------------------------------------
------------------------------
Device Type:Dominion KSX2     Model:DKSX2_188
Device Name:YongKSX2          FW Version:1.0.0.5.6321
SN:AE17950009
IP Address:192.168.59.202     Idle Timeout:0min
IP Address:192.168.59.202     Idle Timeout:0min
Port Port                         Port Port   Port
No.  Name                         Type Status Availability
1  - Dominion_KSX2_Port1 Not Available down   idle
2  - Dominion_KSX2_Port3 Not Available down   idle
3  - Dominion_KSX2_Port4 Not Available down   idle
4  - Dominion_KSX2_Port5 Not Available down   idle
5  - YongFedora7        VM           up     idle
6  - Yong-Laptop-XP     Not Available down   idle
7  - Dominion_KSX2_Port8 Not Available down   idle
8  - Serial Port 1      Serial       up     idle
9  - Serial Port 2      Serial       up     idle
10  - Serial Port 3      Serial       up     idle
11  - Serial Port 4      Serial       up     idle
12  - Serial Port 5      Serial       up     idle
13  - Serial Port 6      Serial       up     idle
14  - Serial Port 7      Serial       up     idle
15  - Serial Port 8      Serial       up     idle
Current Time:Tue Dec 04 13:22:17 2007
admin>
```

```
login as:Janet
Password:
Authentication successful.

------------------------------------------------------
-------------
Welcome to the KSX II  [Model:KSX2]
UnitName:KSX II       FirmwareVersion:3.0.0.5.1
Serial:WACEA00008
IP Address:192.168.51.194  UserIdletimeout:99min
------------------------------------------------------
--------------
Port Port                         Port Port
No.  Name                        No.  Name
1  - Port1 [U]                    2  - Port2 [U]
3  - Port3 [U]                    4  - Port4 [U]
Current Time:Wed Sep 20 16:05:50 2006
Janet >
```

CLI の画面操作

CLI を使用する前に、CLI の画面操作と構文について理解しておくことが重要です。また、CLI の使用を簡素化するキー入力の組み合わせについても、理解しておく必要があります。

コマンドのオート コンプリート

CLI にはオート コンプリート機能（コマンドの一部を入力すると、残りの部分が自動入力される機能）が備わっています。先頭の数文字を入力した後、Tab キーを押します。入力した文字列で始まるコマンドの候補が 1 つしかない場合、オート コンプリート機能によって残りの部分が自動入力されます。

- 入力した文字列で始まるコマンドの候補が見つからない場合、そのレベルに対する有効な入力候補が表示されます。
- 入力した文字列で始まるコマンドの候補が複数個見つかった場合、すべての入力候補が表示されます。

この場合、コマンドの続きを入力して候補が 1 つだけになるようにし、Tab キーを押してコマンドを自動入力します。

CLI 構文: ヒントとショートカット キー

ヒント

- コマンドは、アルファベット順に表示されています。
- コマンドでは、大文字と小文字は区別されません。
- パラメータ名は、アンダスコアを含まない 1 つの単語です。
- コマンドに対して引数を指定しない場合、そのコマンドに対する現在の設定値が指定されていると見なされます。
- コマンドの後ろに疑問符 (?) を指定した場合、そのコマンドに対するヘルプが表示されます。
- 縦線（|）は、任意指定または必須指定のキーワードまたは引数における、選択肢を意味します。

ショートカット

- 末尾のエントリを表示するには、上方向キーを押します。
- 最後に入力した文字を削除するには、Backspace キーを押します。
- 誤ったパラメータを入力した場合にコマンドを終了またはキャンセルするには、Ctrl キーを押しながら C キーを押します。
- コマンドを実行するには、Enter キーを押します。
- コマンドの入力中に残りの部分を自動入力するには、Tab キーを押します。たとえば、Admin Port > プロンプトで Conf と入力した後に Tab キーを押すと、`Admin Port > Config >` プロンプトが表示されます。

すべての CLI レベルで使用できるコマンド

次の表に、すべての CLI レベルで使用できるコマンドを示します。これらのコマンドは、CLI の画面操作にも役立ちます。

コマンド	説明
top	CLI 階層の最上位レベル、つまり username プロンプトに戻ります。
history	KSX II の CLI で入力した最後の 200 個のコマンドが表示されます。
help	CLI 構文の概要が表示されます。
quit	1 レベル上に戻ります。
logout	ユーザ セッションが終了し、ユーザがログオフされます。

CLI を使用した初期設定

注: この項で説明する、CLI を使用した手順の実行は任意です。KSX II ローカル コンソールで同じ設定作業を実行できるからです。詳細については、「最初に行う作業」を参照してください。

KSX II は、デフォルト値に設定された状態で工場から出荷されます。初めて電源を入れて接続を行う際、次のとおりに基本パラメータ値を設定し、ネットワーク上から KSX II に安全にアクセスできるようにする必要があります。

1. 管理者パスワードを再設定します。KSX II は、すべてのデバイスに同じデフォルト パスワードが設定された状態で出荷されます。したがって、セキュリティ侵害を回避するため、管理者パスワードをデフォルトの raritan から変更する必要があります。新しいパスワードは、KSX II の管理者になるユーザが決めます。
2. IP アドレス、サブネット マスク、およびデフォルト ゲートウェイの値を設定し、リモート アクセスできるようにします。

パラメータ値を設定する

パラメータ値を設定するには、管理者権限でログオンする必要があります。CLI 階層の最上位である `username >` プロンプトが表示されます。初期設定を行うため、`admin` と入力します。top コマンドを入力し、最上位レベルに戻ります。

注: admin 以外のユーザ名でログオンした場合、admin の代わりにそのユーザ名が表示されます。

ネットワーク パラメータの設定

ネットワーク パラメータ値を設定するには、interface コマンドを使用します。

```
admin > Config > Network > interface ipauto none ip
192.168.151.12 mask 255.255.255.0 gw 192.168.151.1 mode
auto
```

このコマンドが受け付けられると、KSX II との接続が自動切断されます。新たに設定した IP アドレス、および、「パラメータ値を設定する」で作成したユーザ名とパスワードを使用して、KSX II に再接続します。

重要: パスワードを忘れてしまった場合は、KSX II の背面にあるリセット ボタンを押し、出荷時設定に戻す必要があります。この場合、初期設定作業を再度実行する必要があります。

これで KSX II の基本情報が設定されたので、SSH またはグラフィカル ユーザ インタフェース (GUI) を使用してリモート アクセスすることや、ローカル シリアル ポートを使用してローカル アクセスすることができます。管理者は、ユーザ、グループ、サービス、セキュリティ、およびシリアル ポートを設定する必要があります。シリアル ポートは、シリアル ターゲットを KSX II に接続するためのポートです。

CLI プロンプト

CLI プロンプトは、現在のコマンド レベルを意味しています。プロンプトのルート部分はログオン名です。端末エミュレーション ソフトウェアを使用して管理用シリアル ポートに直接接続している場合、コマンドのルート部分は Admin Port になります。

```
admin >
```

Telnet または SSH で接続している場合、コマンドのルート部分は admin になります。

```
admin > config > network >
```

0

CLI コマンド

下の表は、使用可能なすべての CLI コマンドの一覧とその説明です。

コマンド	説明
config	ポート設定コマンド [Configuration] (設定) メニューに切り替えます。
connect	ポートに接続します。
diagnostics	diagnostics コマンド メニューに切り替えます。
help	CLI 構文の概要が表示されます。
history	現在のセッションのコマンド ライン履歴を表示します。
interface	KSX II のネットワーク インタフェースを設定します。
listports	使用可能なポートを一覧表示します。
logout	現在の CLI セッションを終了し、ログオフします。
name	デバイス名やホスト名を表示、または変更します。

コマンド	説明
config	ポート設定コマンド [Configuration] (設定) メニューに切り替えます。
quit	前のコマンドに戻ります。
userlist	ユーザを一覧表示します。

セキュリティ上の問題

コンソール サーバにおけるセキュリティを確保する際に検討すべき点は、次のとおりです。

- 運用担当者用コンソールと KSX II との間で送受信されるデータ トラフィックを暗号化する。
- ユーザに対して認証を行い、また、ユーザに付与する権限を制限する。
- セキュリティ プロファイルを設定する。

KSX II にはこの 3 つの機能がすべて備わっています。ただし、設定作業は運用開始前に済ませておく必要があります。

ターゲット接続と CLI

KSX II の目的は、connect コマンドを使用して、承認されたユーザとさまざまなターゲット デバイスとの接続を確立することです。ターゲットに接続する前に、ターミナル エミュレーションとエスケープ シーケンスを設定する必要があります。ターゲットが切断された場合、適切な切断メッセージが表示されます。KSX II では、ユーザ間でポートを共有することもできます。

ターゲットでのエミュレーションの設定

▶ **ターゲットでエミュレーションを設定するには、以下の手順に従います。**

- ホスト上で使用中のエンコードがターゲット デバイスで設定されているエンコードと一致することを確認します。たとえば、Sun™ Solaris™ サーバの文字セットが ISO8859-1 に設定されている場合は、ターゲット デバイスも ISO8859-1 に設定する必要があります。

注: Raritan は ISO9660 形式を標準でサポートしています。ただし、その他の CD-ROM 拡張でも動作します。

- KSX II シリアル ポートに接続されているターゲット ホストのターミナル エミュレーションが VT100、VT220、VT320 または ANSI であることを確認します。

ほとんどの UNIX® システムでは、TERM=vt100 (または vt220|vt320|ansi) をエクスポートすることによって UNIX ターゲット デバイス上の優先ターミナル エミュレーション タイプを設定します。HP-UX® サーバのターミナル タイプが VT100 に設定されている場合、Access Client も VT100 に設定する必要があります。

KSX II 上のターミナル エミュレーション設定が、特定のターゲット デバイスのポート設定と適切に関連付けられます。Telnet や SSH クライアントなどのクライアント ソフトウェアのターミナル エミュレーションの設定が、ターゲット デバイスをサポートできることを確認します。

CLI を使用したポート共有

アクセス クライアント ユーザは他の認証済みおよび認可済みのユーザとポートを共有できます。共有対象ユーザがアクセス クライアント ユーザ (RSC) であるか、SSH/Telnet ユーザであるかは関係ありません。ポート共有は、アプリケーションのトレーニングやトラブルシューティングに利用されます。

- ユーザが書き込みアクセスまたは読み取り専用アクセスを持っているかは、ポート共有セッション中のどの時点でもリアルタイムに通知されます。
- 書き込み許可を持っているユーザは、ポートに書き込みアクセスを要求できます。

KSX II コンソール サーバ設定用コマンドを使用する

注: SSH 接続、Telnet 接続、ローカル ポート接続のどの場合でも、CLI コマンドは同じです。

network コマンドは、Configuration メニューで使用できます。

ネットワークを設定する

network メニューのコマンドを使用して、KSX II のネットワーク インタフェースを設定します。

コマンド	説明
interface	KSX II のネットワーク インタフェースを設定します。
name	ネットワーク名を設定します。
ipv6	IPv6 のネットワーク パラメータ値を取得および

コマンド	説明
	設定します。

interface コマンド

interface コマンドを使用して、KSX II のネットワーク インタフェースを設定します。interface コマンドの構文は次のとおりです。

```
interface [ipauto <none|dhcp>] [ip <ipaddress>] [mask <subnetmask>] [gw <ipaddress>] [mode <mode>]

Ethernet パラメータ値を設定/取得します。

ipauto <none|dhcp>: IP アドレスを自動設定するかどうか (none/dhcp)。

ip <ipaddress>: IP アドレス。

mask <subnetmask>: サブネット マスク。

gw <ipaddress>: デフォルト ゲートウェイ。

mode <mode>: Ethernet モードを設定 (auto/10hdx/10fdx/100hdx/100fdx/1000fdx)。
```

interface コマンドの例

次のコマンドを実行すると、インタフェース番号 1 が有効になり、IP アドレス、サブネット マスク、およびデフォルト ゲートウェイの値が設定され、Ethernet モードが自動検出に設定されます。

```
Admin > Config > Network > interface ipauto none ip 192.16.151.12 mask 255.255.255.0 gw 192.168.51.12 mode auto
```

name コマンド

name コマンドを使用して、ネットワーク名を設定します。name コマンドの構文は次のとおりです。

```
name [devicename <devicename>] [hostname <hostname>]
```

デバイス名の設定

```
devicename <devicename>: デバイス名。
hostname <hostname>: 優先ホスト名 (DHCP 使用時のみ)。
```

name コマンドの例

次のコマンドを実行すると、ネットワーク名が設定されます。

```
Admin > Config > Network > name devicename My-KSX2
```

connect コマンド

connect コマンドにより、ポートやその履歴にアクセスできます。

コマンド	説明
connect	ポートに接続します。ポートのサブメニューには、エスケープ キー シーケンスで移動できます。
clearhistory	このポートの履歴バッファをクリアします。書き込みアクセスを持つユーザだけが実行できます。
clientlist	ポート上のすべてのユーザを表示します。
close	このターゲット接続を閉じます。
gethistory	このポートの履歴バッファを表示します。読み取り専用許可しか持たないユーザは利用できません。
getwrite	ポートの書き込みアクセスを取得します。読み取り専用許可しか持たないユーザは利用できません。
help	コマンドの概要が表示されます。
history	現在のセッションのコマンド ライン履歴を表示します。
powerstatus	電源ステータス ポートを照会します。電源管理の許可を持たないユーザは利用できません。

コマンド	説明
powertoggle	ポートの電源のオンとオフを切り替えます。電源管理の許可を持たないユーザは利用できません。操作できるのは、関連付けられたシリアル ターゲットの電源だけです。
quit	このターゲット接続を閉じます。
return	ターゲット セッションに戻ります。
sendbreak	接続されたターゲットに切断を送信します。読み取り専用許可しか持たないユーザは利用できません。
writelock	ポートの書き込みアクセスをロックします。読み取り専用許可しか持たないユーザは利用できません。
writeunlock	ポートの書き込みアクセスをロック解除します。読み取り専用許可しか持たないユーザは利用できません。

ipv6 コマンド

ipv6 コマンドを使用して、IPv6 関連のネットワーク パラメータ値の設定と取得を行います。

```
Ipv6_interface mode enable ipauto none ip
2001:db8:290c:1291::17 prefixlen 128 gw
2001:db8:290c:1291::1
```

Ch 13 KSX II ローカル コンソール

この章の内容

概要 264
KSX II ローカル コンソールを使用する... 265
KSX II ローカル コンソール インタフェース 265
セキュリティと認証.. 266
ローカル コンソールのスマート カード アクセス.......................... 267
ローカル コンソールの USB プロファイル オプション.................. 268
有効な解像度.. 269
[Port Access] (ポート アクセス) ページ (ローカル コンソール サーバ ディスプレイ).. 270
サーバ表示.. 272
ホット キーと接続キー.. 273
各言語に対して KSX II でサポートされているキーボード................ 274
Sun サーバへのアクセス時に使用できる特別なキー組み合わせ 276
ターゲット サーバにアクセスする 276
KSX II ローカル コンソールの画面に切り替える 277
ローカル ポートの管理.. 277
リセット ボタンを使用して KSX II をリセットする 282

概要

KSX II のローカル ポートにコンピュータを接続して KSX II ローカル コンソールを使用することにより、設置場所で管理作業を行うことができます。この KSX II ローカル コンソールの特徴は、ブラウザを使用する、という点であり、サーバをすばやく切り替えることができます。KSX II のローカル コンソールでは、接続されたサーバへの直接的なアナログ接続が可能です。これにより、サーバのキーボード、マウス、ビデオ ポートに直接接続しているようなパフォーマンスが期待できます。また、KSX II ローカル コンソールには、KSX II リモート コンソールと同等の管理機能が備わっています。

KSX II ローカル コンソールを使用する

ユーザが同時接続可能

KSX II ローカル コンソールを使用する場合、接続されている各 KVM ターゲット サーバへの独立したアクセス パスが設定されます。シリアル接続の場合、アクセス パスは共有されます。つまり、KSX II ローカル コンソールを使用している最中でも、他ユーザがネットワーク経由で KSX II に同時接続できます。また、リモート ユーザが KSX II に接続している最中でも、KSX II ローカル コンソールを使用してラックからサーバに同時接続できます。

KSX II ローカル コンソール インタフェース

サーバ ラックに設置した KSX II の場合は、KSX II ローカル コンソールを介して、標準 KVM 管理を行います。KSX II ローカル コンソールは接続されたサーバへの直接 KVM (アナログ) 接続を提供し、これにより、サーバのキーボード、マウス、ビデオ ポートに直接接続しているかのように機能することが可能になります。また、KSX II はシリアル ターゲットへのアクセス時にターミナル エミュレーションも提供します。

KSX II ローカル コンソールと KSX II リモート コンソールのグラフィカル ユーザ インタフェースには、多くの類似点があります。相違点については、ヘルプに記載されています。

[KSX II Local Console Factory Reset] (KSX II ローカル コンソール ファクトリ リセット) オプションは、KSX II ローカル コンソールには用意されていますが、KSX II リモート コンソールには用意されていません。

セキュリティと認証

KSX II ローカル コンソールを使用するには、まず有効なユーザ名とパスワードで認証を受ける必要があります。KSX II には認証機能とセキュリティ機能が備わっています。これらの機能は、ネットワークから接続するユーザとローカル ポートから接続するユーザの両方に対して有効です。ユーザは、どちらの方法で接続する場合でも、アクセス権限を持っているサーバにしかアクセスできません。サーバ アクセスとセキュリティに関する設定情報を指定する手順については、「ユーザ管理」を参照してください。

KSX II が外部認証サービス（LDAP/LDAPS、RADIUS、または Active Directory）を使用するように設定されている場合、ユーザが KSX II ローカル コンソールを使用して接続する際でも、外部認証サービスによって認証が行われます。

注: KSX II ローカル コンソールを使用して接続しようとするユーザに対して認証を行わないように、設定することもできます。ただし、この方法は安全な環境でのみ使用することを推奨します。

KSX II ローカル コンソールを使用するには

1. キーボード、マウス、およびモニタを、KSX II の背面にあるローカル ポートに接続します。
2. KSX II を起動します。KSX II ローカル コンソール画面が表示されます。

ローカル コンソールのスマート カード アクセス

ローカル コンソールでスマート カードを使用してサーバにアクセスするには、KSX II に搭載されているいずれかの USB ポートを使用して USB スマート カード リーダーを KSX II に接続します。

スマート カード リーダーは、KSX II に接続したり KSX II から取り外したりすると、KSX II によって自動検出されます。

サポートされているスマート カードおよびシステム要件の一覧については、「***サポートされているスマート カード リーダーとサポートされていないスマート カード リーダー*** 『*310*p. 』」および「***スマート カードの最小システム要件*** 『*311*p. 』」を参照してください。

カード リーダーおよびスマート カードをターゲット サーバにマウントすると、サーバはそれらのリーダーやカードが直接接続されているかのように動作します。

スマート カードまたはスマート カード リーダーを取り外すと、ターゲット サーバの OS で設定されているカードの取り外しポリシーに従って、ユーザ セッションがロックされるか、またはユーザがログアウトされます。

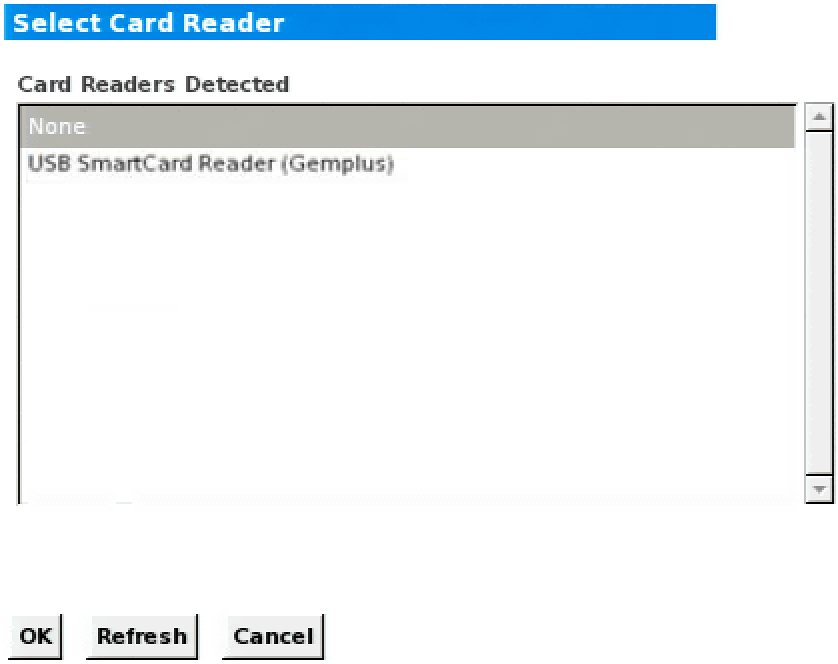
KVM セッションが切断されるか、または新しいターゲットに切り替えたために KVM セッションが終了した場合、スマート カード リーダーはターゲット サーバから自動的にマウント解除されます。

► **KSX II ローカル コンソールからスマート カード リーダーをターゲットにマウントするには、以下の手順に従います。**

1. デバイスに搭載されているいずれかの USB ポートを使用して、USB スマート カード リーダーを KSX II に接続します。接続すると、スマート カード リーダーは KSX II によって検出されます。
2. ローカル コンソールで [Tools] (ツール) をクリックします。
3. [Card Reader Detected] (検出されたカード リーダー) リストからスマート カード リーダーを選択します。スマート カード リーダーをマウントしない場合は、リストから [None] (なし) を選択します。
4. [OK] (OK) をクリックします。スマート カード リーダーを追加すると、操作が正常に完了したことを示すメッセージがページに表示されます。ページの左パネルの [Card Reader] (カード リーダー) に、状態として [Selected] (選択) または [Not Selected] (未選択) が表示されます。

▶ **[Card Readers Detected] (検出されたカード リーダー) リストを更新するには、以下の手順に従います。**

- 新しいスマート カードがマウントされた場合は、[Refresh] (更新) をクリックします。[Card Readers Detected] (検出されたカード リーダー) リストが更新され、新しく追加されたスマート カード リーダーが表示されます。



ローカル コンソールの USB プロファイル オプション

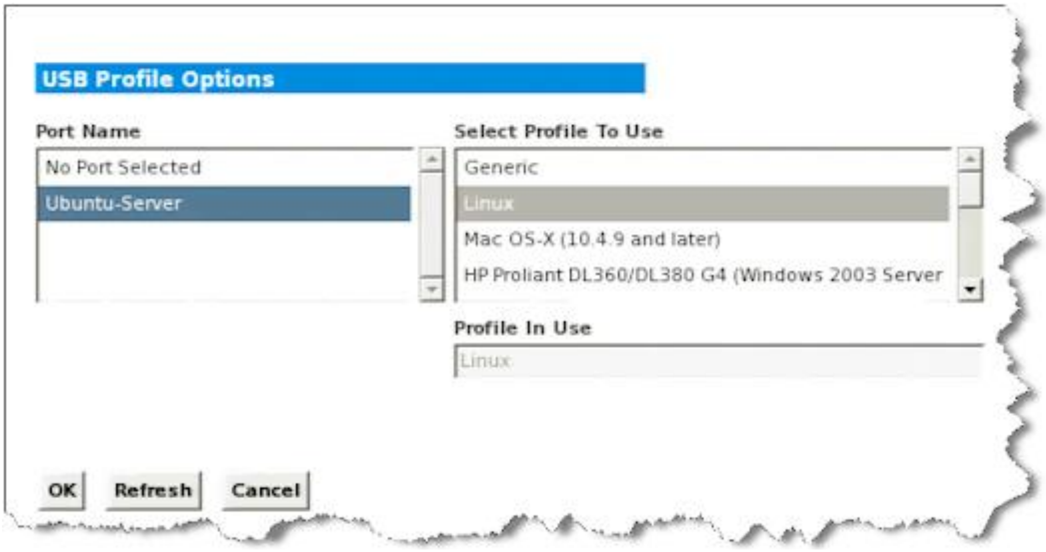
[Tools] (ツール) ページの [USB Profile Options] (USB プロファイル オプション) セクションで、ローカル ポートに対する USB プロファイルを選択できます。

プロファイルを適用可能なポートが [Port Name] (ポート名) フィールドに表示されます。ポートを選択すると、そのポートに適用可能なプロファイルが [Select Profile To Use] (使用するプロファイルを選択) フィールドに表示されます。ポートに対して選択したプロファイルは、[Profile In Use] (使用中のプロファイル) フィールドに表示されます。

▶ **USB プロファイルをローカル コンソール ポートに適用するには**

1. [Port Name] (ポート名) フィールドで、USB プロファイルを適用するポートを選択します。
2. [Select Profile To Use] (使用するプロファイルを選択) フィールドで、そのポートに適用するプロファイルを選択します。

3. [OK] (OK) をクリックします。その USB プロファイルがローカルポートに適用され、また、[Profile In Use] (使用中のプロファイル) フィールドに表示されます。



有効な解像度

KSX II ローカル コンソールは次の解像度に対応しており、さまざまなモニタで適切に表示されます。

- 800x600
- 1024 x 768
- 1280 x 1024

これらの各解像度について、60 Hz と 75 Hz のリフレッシュ レートがサポートされています。

[Port Access] (ポート アクセス) ページ (ローカル コンソール サーバ ディスプレイ)

KSX II ローカル コンソールにログオンすると、[Port Access] (ポート アクセス) ページが開きます。このページには、KSX II のポート、各ポートに接続されている KVM ターゲット サーバ、および各ターゲット サーバのステータスと稼動状態が一覧表示されます。

また、KSX II で設定されているブレード筐体も表示されます。

ブレード サーバは、[Port Access] (ポート アクセス) ページ上の展開可能な階層リストに表示されます。階層のルートはブレード シャーシで、個別のブレードはルートの下にラベルが付けられて表示されます。個別のブレードを表示するには、ルート シャーシの横の展開矢印アイコン ▶ を使用します。

注: ブレード シャーシを階層順に表示するには、ブレード サーバ シャーシにブレード シャーシのサブタイプを設定する必要があります。

[View by Group] (グループ別表示) タブには、ブレード シャーシ、「標準の」ポート グループ、およびデュアル ビデオ ポート グループが表示されます。グループの横の展開矢印アイコン ▶ クリックすると、ポート グループに割り当てられたポートが表示されます。

▶ [Port Access] (ポート アクセス) ページを使用するには、以下の手順に従います。

1. KSX II ローカル コンソールにログインします。

   デフォルトでは、情報はポート番号別に並べられますが、表示されているいずれかの列の見出しをクリックすると、その列で並べ替えて表示されます。

   - [Port Number] (ポート番号) - 1 から KSX II デバイスで使用できるポートの合計数までの番号が振られています。
   - [Port Name] (ポート名) - KSX II ポートの名前です。最初は、「Dominion-KX2-Port#」に設定されていますが、わかりやすい名前に変更できます。[Port Name] (ポート名) のリンクをクリックすると、[Port Action] (ポート アクション) メニューが表示されます。

   注: ポート (CIM) 名にアポストロフィ (”’”) を使用することはできません。

   - [ステータス]: 標準サーバのステータスは [アップ] または [ダウン] のどちらかです。
   - [タイプ]: サーバまたは CIM のタイプです。ブレード シャーシの場合、タイプは、[ブレード シャーシ]、[ブレード] 、[ブレードシャーシ管理] 、および [ブレードシャーシ URL] です。

- [Availability] (可用性) – 可用性は、[Idle] (アイドル)、[Connected] (接続済み)、[Busy] (ビジー)、または [Unavailable] (使用不可能) のいずれかです。ブレード サーバの場合、そのサーバへの接続が存在する際の可用性は、[shared] (共有) または [exclusive] (排他) です。

2. 必要に応じてビューを切り替えます。[View by Port] (ポート別に表示) タブをクリックすると、情報がポート別に表示されます。[View by Group] (グループ別に表示) タブをクリックすると、情報がポート グループ別に表示されます。
   - [View by Group] (グループ別に表示) ビューには、ポート番号、ポート名、ステータス、タイプ、稼動状態の各列に加え、グループ列も表示されます。この列には、使用可能なポート グループが表示されます。
3. アクセスするターゲット サーバのポート名をクリックします。[ポート アクション] メニューが表示されます。使用可能なメニュー オプションの詳細については、「*[ポート アクション] メニュー*『*53*p. の *"[Port Action] (ポート アクション) メニュー"*参照 』」を参照してください。
4. [ポート アクション] メニューから、目的のメニュー コマンドを選択します。

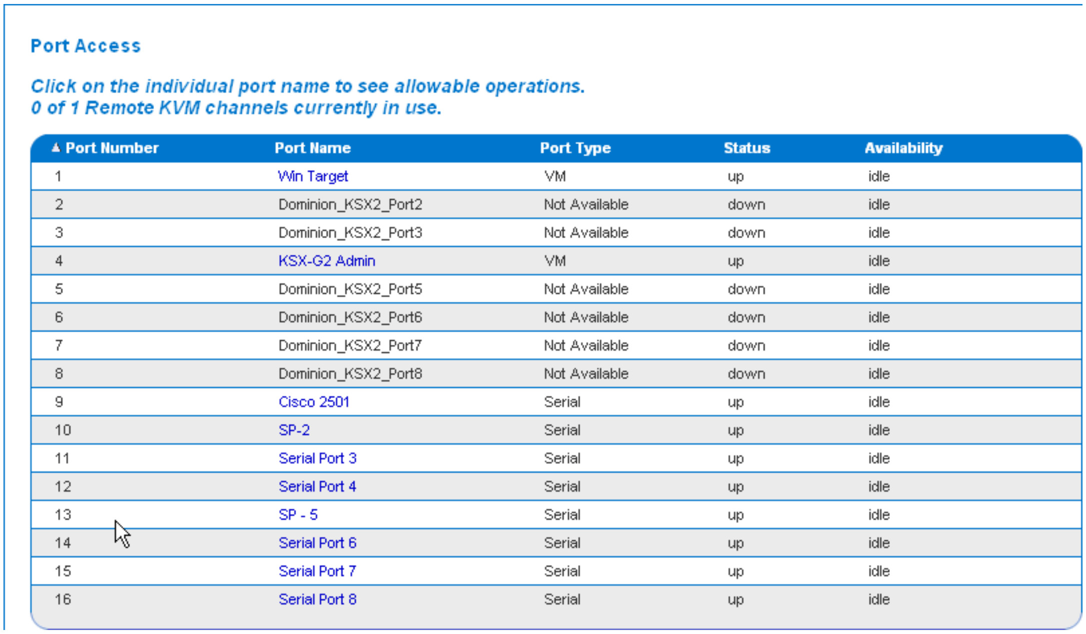
▶ 表示順を変更したり同じページにさらにポートを表示したりするには、以下の手順に従います。

1. 並べ替えで基準にする列の見出しをクリックします。その列に基づいて KVM ターゲット サーバのリストが並べ替えられます。

- [1 ページ当たりの行] に、ページに表示するポート数を入力し、[設定] をクリックします。

サーバ表示

KSX II ローカル コンソールにログオンすると、[Port Access] (ポート アクセス) ページが開きます。このページには、KSX II のポート、KVM ターゲット サーバ、およびシリアル サーバのステータスと稼動状態が一覧表示されます。



Port Access

Click on the individual port name to see allowable operations.
0 of 1 Remote KVM channels currently in use.

▲ Port Number	Port Name	Port Type	Status	Availability
1	Win Target	VM	up	idle
2	Dominion_KSX2_Port2	Not Available	down	idle
3	Dominion_KSX2_Port3	Not Available	down	idle
4	KSX-G2 Admin	VM	up	idle
5	Dominion_KSX2_Port5	Not Available	down	idle
6	Dominion_KSX2_Port6	Not Available	down	idle
7	Dominion_KSX2_Port7	Not Available	down	idle
8	Dominion_KSX2_Port8	Not Available	down	idle
9	Cisco 2501	Serial	up	idle
10	SP-2	Serial	up	idle
11	Serial Port 3	Serial	up	idle
12	Serial Port 4	Serial	up	idle
13	SP - 5	Serial	up	idle
14	Serial Port 6	Serial	up	idle
15	Serial Port 7	Serial	up	idle
16	Serial Port 8	Serial	up	idle

当初 KVM とシリアル ターゲット サーバはポート番号順に並んでいますが、列のいずれかを基準に表示順を変更できます。

- [Port Number] (ポート番号) – 1 から KSX II で使用できるポートの合計数までの番号が振られています。
- [Port Name] (ポート名) – KSX II ポートの名前です。最初は、「Dominion-KSX II-Port#」に設定されていますが、わかりやすい名前に変更できます。[Port Name] (ポート名) のリンクをクリックすると、[Action] (アクション) メニューが開きます。
- [Port Type] (ポート タイプ) – [Serial] (シリアル)、[KVM]、[Power Strip] (電源タップ)、[Not Available] (使用不可)。

注: ポート (CIM) 名にアポストロフィ (" ' ") を使用することはできません。

- [Status] (ステータス) – ステータスは [up] (アップ) または [down] (ダウン) のどちらかです。

▶ ソート順を変更するには、以下の手順に従います。

- 並び替えで基準にする列の見出しをクリックします。その列に基づいて KVM ターゲット サーバのリストが並べ替えられます。

ホット キーと接続キー

KSX II ローカル コンソールの画面は、現在アクセスしているターゲット サーバの画面に完全に置き換えられます。ターゲット サーバから切断し、ローカル コンソールの画面に戻るには、ホット キーを使用します。

接続キーは、ターゲット サーバに接続したり、ターゲット サーバを切り替えたりする際に使用します。

ターゲット サーバの画面が表示されているときにホットキーを使用することにより、KSX II ローカル コンソールの画面をすばやく開くことができます。

「ローカル コンソールからの KSX II ローカル ポートの設定」を参照してください。

接続キーの例

標準型サーバの場合

接続キーを押したときのアクション	キー組み合わせの例
KSX II ローカル コンソールからポートに接続する	KSX II ローカル コンソールからポート 5 に接続するには • 左 Alt キーを押す → 5 キーを押して離す → 左 Alt キーを離す
ポートを切り替える	ポート 5 からポート 11 に切り替えるには • 左 Alt キーを押す → 1 キーを押して離す → 1 キーを押して離す → 左 Alt キーを離す
ターゲット サーバから切断し、KSX II ローカル コンソールの画面に戻る	ポート 11 から切断し、KSX II ローカル コンソールの画面（ターゲット サーバに接続する時に開いていたページ）に戻るには • Scroll Lock キーをすばやく 2 回押す

ブレード シャーシの場合

接続キーを押したときのアクション	キー組み合わせの例
KSX II ローカル コンソールからポートに接続する	ポート 5 のスロット 2 に接続するには • 左 Alt キーを押す → 5 キーを押して離す → 2 キーを押して離す → 左 Alt キーを離

標準型サーバの場合 接続キーを押したときのアクション	キー組み合わせの例
	す
ポートを切り替える	ポート 5 のスロット 2 からポート 5 のスロット 11 に切り替えるには • 左 Alt キーを押す → 5 キーを押して離す → 1 キーを押して離す → 1 キーを押して離す → 左 Alt キーを離す
ターゲット サーバから切断し、KSX II ローカル コンソールの画面に戻る	ポート 11 のスロット 11 から切断し、KSX II ローカル コンソールの画面 (ターゲット サーバに接続する時に開いていたページ) に戻るには • Scroll Lock キーをすばやく 2 回押す

各言語に対して KSX II でサポートされているキーボード

次の表に、各言語に対して KSX II でサポートされているキーボードを示します。

注:中国語、日本語、および韓国語は、表示しかできません。現時点では、これらの言語を入力することはできません。アメリカ英語以外のキーボードの詳細については、「留意事項」を参照してください。

注:Linux 環境で作業する場合は、system-config-keyboard を使用して言語を変更することをお勧めします。

言語	地域	キーボード レイアウト
US 英語	米国および大半の英語圏の諸国: カナダ、オーストラリア、ニュージーランドなど	US キーボード レイアウト
US インターナショナル	米国および大半の英語圏の諸国: オランダなど	US キーボード レイアウト
UK 英語	英語 (イギリス)	UK レイアウト キー

言語	地域	キーボード レイアウト
		ボード
繁体字中国語	香港、中国（台湾）	繁体字中国語
簡体字中国語	中国	簡体字中国語
韓国語	韓国	Dubeolsik ハングル
日本語	日本	JIS キーボード
[French]（フランス語）	フランス	フランス語 (AZERTY) レイアウト キーボード
[German]（ドイツ語）	ドイツおよびオーストリア	ドイツ語キーボード (QWERTZ レイアウト)
[French]（フランス語）	ベルギー	ベルギー語（ベルギー）
ノルウェー語（ノルウェー）	ノルウェー	ノルウェー語（ノルウェー）
デンマーク語（デンマーク）	デンマーク	デンマーク語（デンマーク）
スウェーデン語（スウェーデン）	スウェーデン	スウェーデン語（スウェーデン）
ハンガリー語	ハンガリー	ハンガリー語
スロベニア語	スロベニア	スロベニア語
イタリア語	イタリア	イタリア語
スペイン語	スペインおよび大半のスペイン語圏の諸国	スペイン語
ポルトガル語	ポルトガル	ポルトガル語

Sun サーバへのアクセス時に使用できる特別なキー組み合わせ

ローカル ポートでは、Sun Microsystems™ サーバの特別なキーに対して、次のキー組み合わせが機能します。これらの特別なキー組み合わせは、Sun ターゲット サーバに接続しているときに使用できます。

Sun サーバのキー	ローカル ポートにおけるキー組み合わせ
Again	Ctrl+ Alt +F2
Props	Ctrl+ Alt +F3
Undo	Ctrl+ Alt +F4
Stop A	Break a
Front	Ctrl+ Alt +F5
Copy	Ctrl+ Alt +F6
Open	Ctrl+ Alt +F7
Find	Ctrl+ Alt +F9
Cut	Ctrl+ Alt +F10
Paste	Ctrl+ Alt +F8
Mute	Ctrl+ Alt +F12
Compose	Ctrl+ Alt + KPAD *
Vol +	Ctrl + Alt + KPAD +
Vol –	Ctrl + Alt + KPAD –
Stop	キー組み合わせなし
電力	キー組み合わせなし

ターゲット サーバにアクセスする

▶ ターゲット サーバにアクセスするには

1. アクセスしたいターゲット サーバのポート名をクリックします。ポート アクション メニューが開きます。
2. ポート アクション メニューの [Connect] (接続) をクリックします。そのターゲット サーバの画面に切り替わります。

KSX II ローカル コンソールの画面に切り替える

重要: KSX II ローカル コンソールのデフォルトのホットキーは、Scroll Lock キーをすばやく 2 回押すことです。

このキー組み合わせを変更するには、[Local Port Settings] (ローカル ポート設定) ページを使用します。オンライン ヘルプの「ローカル コンソールからの KSX II ローカル ポートの設定」を参照してください。

ターゲット サーバの画面から KSX II ローカル コンソールの画面に戻るには

- ホットキーを押します (デフォルトでは Scroll Lock キーをすばやく 2 回押す)。

  ターゲット サーバの画面から KSX II ローカル コンソールの画面に切り替わります。

ローカル ポートの管理

KSX II を管理するには、KSX II ローカル コンソールまたは KSX II リモート コンソールを使用します。KSX II ローカル コンソールには次のページもあります。

- [Factory Reset] (出荷時設定にリセット)
- [Local Port Settings] (ローカル ポート設定)

注: これらのページを使用できるのは、管理者権限を持つユーザだけです。

KSX II ローカル コンソールの [Local Port Settings] (ローカル ポート設定) ページ

[Local Port Settings] (ローカル ポート設定) ページでは、KSX II ローカル コンソールに関するさまざまな設定値をカスタマイズできます。たとえば、キーボード、ローカル ポート ホットキー、画面切り替え遅延、省電力モード、画面解像度設定、ローカル ユーザ認証などに関する設定値をカスタマイズできます。

注: このページは、KSX II ローカル コンソールでのみ使用できます。

ローカル ポートに関する設定値をカスタマイズするには

1. [Device Settings] (デバイス設定) メニューの [Local Port Settings] (ローカル ポート設定) をクリックします。[Local Port Settings] (ローカル ポート設定) ページが開きます。
2. [Keyboard Type] (キーボード タイプ) ボックスの一覧でキーボード タイプを選択します。選択できる項目は次のとおりです。
   - [US] (アメリカ英語)
   - [US/International] (アメリカ英語/国際)

- [United Kingdom] (イギリス英語)
- [French (France)] (フランス語 (フランス))
- [German (Germany)] (ドイツ語 (ドイツ))
- [JIS (Japanese Industry Standard)] (JIS (日本工業規格))
- [Simplified Chinese] (簡体字中国語)
- [Traditional Chinese] (繁体字中国語)
- [Dubeolsik Hangul (Korean)] (Dubeolsik ハングル (韓国))
- [German (Switzerland)] (ドイツ語 (スイス))
- [Norwegian (Norway)] (ノルウェー語 (ノルウェー))
- [Swedish (Sweden)] (スウェーデン語 (スウェーデン))
- [Danish (Denmark)] (デンマーク語 (デンマーク))
- [Belgian (Belgium)] (ベルギー語 (ベルギー))

注: 中国語、日本語、および韓国語は、表示しかできません。現時点では、これらの言語を入力することはできません。

3. [Local Port Hotkey] (ローカル ポート ホットキー) ボックスの一覧でローカル ポート ホットキーを選択します。ローカル ポート ホットキーは、ターゲット サーバの画面が表示されているときに KSX II ローカル コンソールの画面に戻す際に使用します。デフォルト値は [Double Click Scroll Lock] (Scroll Lock キーを 2 回押す) ですが、他のキー組み合わせを選択することもできます。

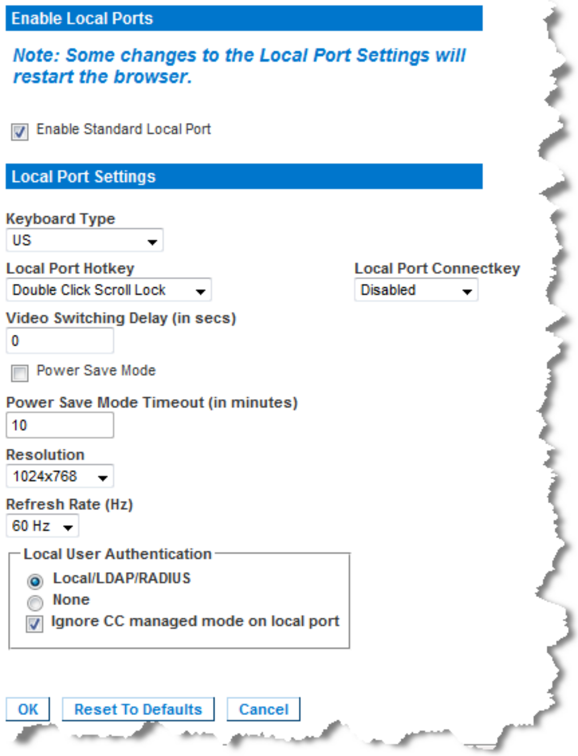
ホットキー	説明
Scroll Lock キーをすばやく 2 回押す	Scroll Lock キーをすばやく 2 回押します。
[Double Click Num Lock] (Num Lock キーを 2 回押す)	Num Lock キーをすばやく 2 回押します。
[Double Click Caps Lock] (Caps Lock キーを 2 回押す)	Caps Lock キーをすばやく 2 回押します。
[Double Click Left Alt key] (左 Alt キーを 2 回押す)	左 Alt キーをすばやく 2 回押します。
[Double Click Left Shift key] (左 Shift キーを 2 回押す)	左 Shift キーをすばやく 2 回押します。
[Double Click Left Ctrl key] (左 Ctrl キーを 2 回押す)	左 Ctrl キーをすばやく 2 回押します。

4. 必要に応じて、[Video Switching Delay (in secs)] (画面切り替え遅延(秒)) ボックスに 0 〜 5 秒の範囲の数値を入力します。通常は「0」と入力します。ただし、一部のモニタでは画面切り替えに時間がかかるので、その場合は適切な値を入力します。
5. 省電力機能を利用する場合、次の手順を実行します。
   a. [Power Save Mode] (省電力モード) チェック ボックスをオンにします。
   b. [Power Save Mode Timeout (in minutes)] (省電力モードのタイムアウト (分)) ボックスに、省電力モードに移行するまでの時間 (単位: 分) を入力します。
6. [Resolution] (解像度) ボックスの一覧で、KSX II ローカル コンソールの画面解像度を選択します。選択できる項目は次のとおりです。
   - 800x600
   - 1024 x 768
   - 1280 x 1024
7. [Refresh Rate (Hz)] (リフレッシュ レート (Hz)) ボックスの一覧でリフレッシュ レートを選択します。選択できる項目は次のとおりです。
   - 60 Hz
   - 75 Hz
8. [Local User Authentication] (ローカル ユーザ認証) でローカル ユーザ認証タイプを選択します。
   - [Local/LDAP/RADIUS] (ローカル/LDAP/RADIUS)これは推奨オプションです。認証の詳細については、「***リモート認証*** 『***41***p. 』」を参照してください。
   - 特別なアクセス用ソフトウェアをインストールする必要はありません。KSX II ローカル コンソールからのアクセスに対して認証は行われません。このオプションは、安全な環境でのみ選択することを推奨します。
9. KSX II が CommandCenter Secure Gateway (CC-SG) の管理下にある場合にローカル ユーザを認証するには、[Ignore CC managed mode on local port] (ローカル ポートからのアクセスを CC-SG の管理対象から除外する) チェック ボックスをオンにします。

注: 最初は [Ignore CC managed mode on local port] (ローカル ポートからのアクセスを CC-SG の管理対象から除外する) チェック ボックスをオフにしていたが、後でローカル ポートからのアクセスを CC-SG の管理対象から除外したくなった場合、CC-SG 側で KSX II を CC-SG の管理対象から除外する必要があります。その後、[Ignore CC managed mode on local port] (ローカル ポートからのアクセスを CC-SG の管理対象から除外する) チェック ボックスをオンにすることができます。

---

10. [OK] をクリックします。



- デフォルトに戻すには、以下の手順に従います。

- [Reset to Defaults] (デフォルトに戻す) をクリックします。

KSX II ローカル コンソールの [Factory Reset] (出荷時設定にリセット) ページ

注: このページは、KSX II ローカル コンソールでのみ使用できます。

KSX II ローカル コンソールでは、さまざまなリセット モードの中から適切なものを選択できます。

*注: 出荷時設定にリセットする前に、監査ログを保存しておくことをお勧めします。出荷時設定にリセットされると、監査ログが削除されます。また、リセット イベントは監査ログに記録されません。監査ログの保存手順については、「**監査ログ** 『228p. の"[Audit Log] (監査ログ)"参照 』」を参照してください。*

- 出荷時設定にリセットするには、以下の手順に従います。

1. [保守] メニューの [出荷時設定にリセット] をクリックします。[出荷時設定にリセット] ページが開きます。

2. リセット モードを選択します。選択できるオプションは次のとおりです。
   - [完全リセット]: すべての設定値を削除し、工場出荷時のデフォルト値にリセットします。KSX II が CC-SG の管理下にある場合は、CC-SG との関連付けが解除されます。このリセット モードではすべての設定値がリセットされるので、リセットしてもよいかどうかを確認するためのダイアログ ボックスが開きます。
   - [ネットワーク パラメータ値をリセット]: KSX II のネットワーク パラメータ値を出荷時設定にリセットします。現在設定されているネットワーク パラメータ値を表示するには、[デバイス設定] メニューの [ネットワーク設定] をクリックします。リセットされる設定値は次のとおりです。
     - IP を自動設定するかどうか
     - IP アドレス
     - サブネット マスク
     - デフォルト ゲートウェイ
     - プライマリ DNS サーバの IP アドレス
     - セカンダリ DNS サーバの IP アドレス
     - 検出ポート
     - 帯域幅制限
     - LAN インタフェースの速度と通信方式 (全二重/半二重)
     - 自動フェイルオーバを有効にするかどうか
     - ping 間隔 (単位: 秒)
     - タイムアウト時間 (単位: 秒)
3. [Reset] (リセット) をクリックして続行します。すべてのネットワーク設定値がリセットされるので、リセットしてもよいかどうかを確認するためのダイアログ ボックスが開きます。
4. [OK] をクリックして続行します。リセットが完了すると、KSX II が自動再起動します。

リセット ボタンを使用して KSX II をリセットする

デバイスの背面パネルにリセット ボタンがあります。誤ってリセットされることがないように､ボタンはパネルに埋め込まれています (このボタンを使用するには、先端が尖った道具が必要です)。

リセット ボタンを押したときに実行される処理については、[Encryption & Share] (暗号化および共有) ページで定義します。「*暗号化および共有*『*213*p. の"*[Encryption & Share] (暗号化および共有)*"参照 』」を参照してください。

*注:出荷時設定にリセットする前に、監査ログを保存しておくことを推奨します。出荷時設定にリセットされると、監査ログが削除されます。また、リセット イベントは監査ログに記録されません。監査ログの保存手順については、「*監査ログ『228*p. の*"[Audit Log] (監査ログ)*"参照 』」*を参照してください。*

▶ デバイスをリセットするには、以下の手順に従います。

1. KSX II の電源を切ります。
2. 先端の尖った道具を使用してリセット ボタンを押し続けます。
3. リセット ボタンを押したまま、KSX II の電源を入れ直します。
4. リセット ボタンを 10 秒間押したままにします。

KSX II がリセットされると、短いビープ音が 2 回鳴り、リセットが完了した旨が通知されます。

Ch 14 モデム設定

この章の内容

UNIX、Linux、および MPC 向け認定モデム 283
低帯域幅の KVM 設定 284
クライアント ダイヤルアップ ネットワーク設定 285
Windows 2000 のダイヤルアップ ネットワーク設定 285
Windows Vista のダイヤルアップ ネットワーク設定......................... 289
Windows XP のダイヤルアップ ネットワーク設定............................ 290

UNIX、Linux、および MPC 向け認定モデム

UNIX®、Linux®、および MPC での動作が保証されたモデムは次のとおりです。

- US Robotics Courier™ 56K Business Modem (Model# 3453B)
- Zoom/Fax Modem 56Kx Dualmode (Model# 2949)
- Zoom 56k v.92/v.90 Modem (Model # 3049)
- US Robotics v.92 56k Fax Modem (Model# 5686)
- US Robotics 56k SportSter® Modem

低帯域幅の KVM 設定

標準的な DSL 接続の低帯域速度で KVM を使用している際に、パフォーマンスを最適化するには、次の設定をお勧めします。この情報は、仮想 KVM と MPC の両方に適用されます。

設定	パフォーマンスを最適化するために行うこと
[Connection speed] (接続速度)	[Connection] (接続)、[Properties] (プロパティ) を選択します。 [Connection Speed] (接続速度) を、クライアントとサーバ間の接続に最適な値に設定します。指定範囲は、384 Kb (低速 DSL の場合) ～ 1MB です。
[Color depth] (色深度)	[Connection] (接続)、[Properties] (プロパティ) を選択します。 [Color Depth] (色深度) をできるだけ小さくします。この値を小さくすればするほど、ターゲット上のビデオ更新の応答が良くなります。 この影響は、ターゲット デスクトップでフォルダを開いたり移動するときに顕著になります。特に、表示の更新が速くなり、接続の使いやすさが総体的に向上します。
[Noise Filter] (ノイズ フィルタ)	[Video] (ビデオ) の [Video Settings] (ビデオ設定) を選択します。 [Noise Filter] (ノイズ フィルタ) を 7 (最高値) に設定します。この設定によって、ターゲットの画面変更で使用される帯域が小さくなるため、ローカルとリモートのマウスの同期が速くなります。
注: 色深度を低く、ノイズ フィルタを高く設定すると、ビデオの画質が粗くなります。ただし、このトレードオフは、マウスの同期とビデオの更新が速くなって総体的には使いやすさが向上することで相殺されます。	
[Smoothing] (スムージング)	[Connection] (接続)、[Properties] (プロパティ) を選択します。 [Smoothing] (スムージング) を高く設定します。これにより、表示されるビデオ ノイズが減少し、ターゲット ビデオの画質が向上します。

設定	パフォーマンスを最適化するために行うこと
[Auto Color Calibration] (自動色調整)	[Video] (ビデオ) の [Auto-sense Video Settings] (ビデオ設定の自動検出) を選択します。 [Automatic Color Calibration] (自動色調整) チェックボックスをオフにして、このオプションを無効にします。
[Quick sense video mode] (クイック検出ビデオ モード)	[Video] (ビデオ)、[Video Settings] (ビデオ設定) を選択して、[Settings] (設定) ダイアログを開きます。 [Quick sense video mode] (クイック検出ビデオ モード) ラジオ ボタンを選択して、このオプションを有効にします。

クライアント ダイヤルアップ ネットワーク設定

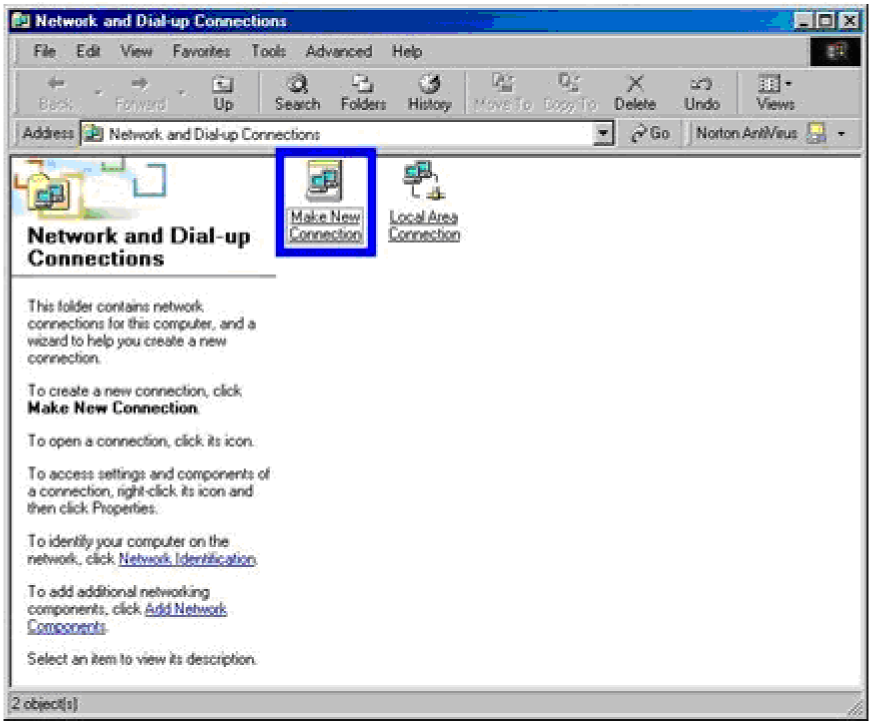
KSX II で使用するために Microsoft Windows® のダイヤルアップ ネットワークを設定すると、PC を KSX II と同じ PPP ネットワークに属するように設定できます。ダイヤルアップ接続が確立されると、KSX II への接続は、Web ブラウザから PPP サーバの IP をポイントすることで行えます。モデム インストールのガイドラインは、次のクライアント ベース システム用に提供されています。

- Windows 7®
- Windows XP®
- Windows Vista®

Windows 2000 のダイヤルアップ ネットワーク設定

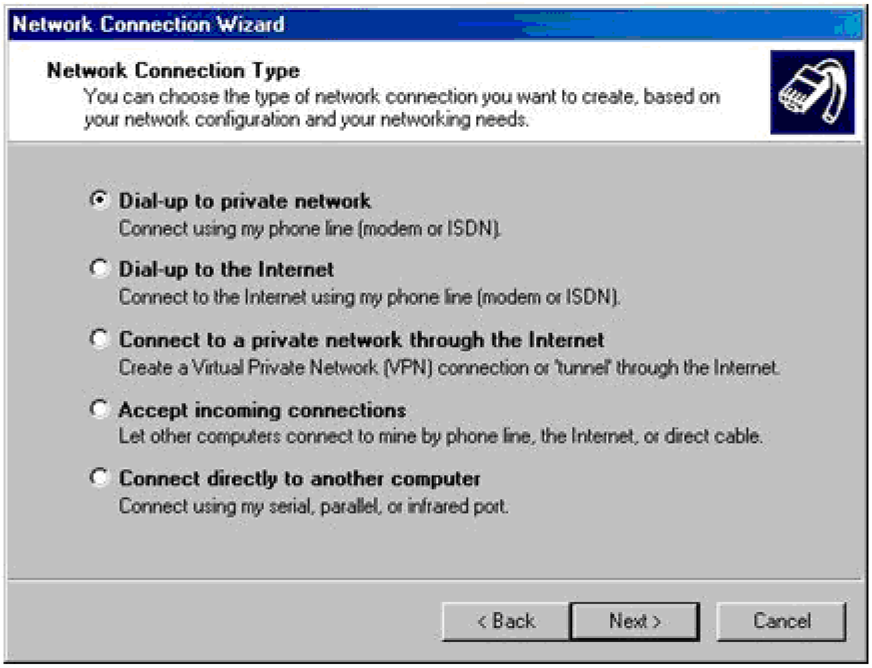
1. [スタート]、[プログラム]、[アクセサリ]、[通信]、[ネットワークとダイヤルアップ接続] の順に選択します。

2. ［ネットワークとダイヤルアップ接続］ウィンドウが表示されたら、［新規接続の作成］アイコンをダブルクリックします。

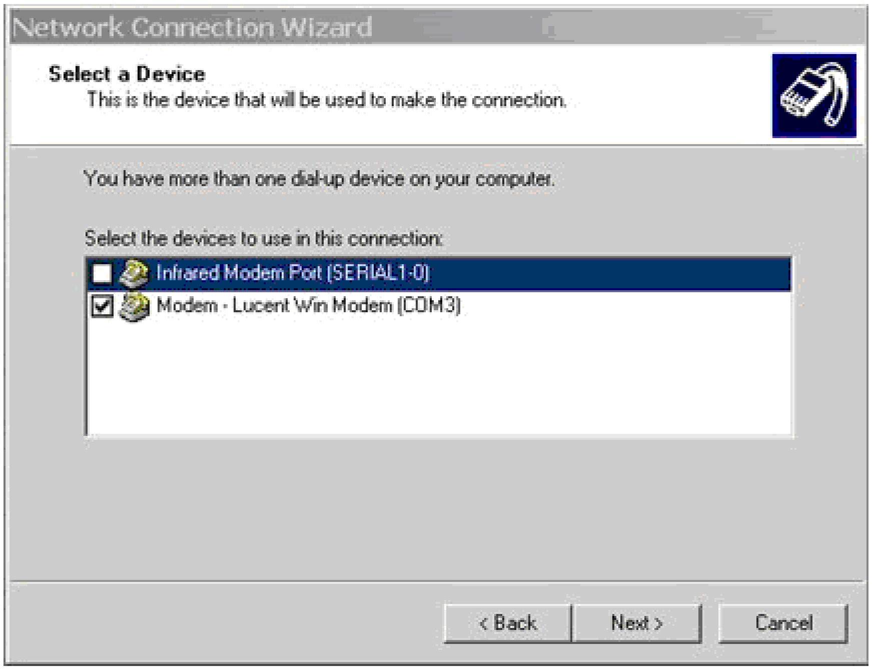


3. ［次へ］をクリックして、［ネットワーク接続ウィザード］ダイアログボックスの手順に従います。これからダイヤルアップ ネットワークのプロファイルを作成します。

4. ［プライベート ネットワークにダイヤルアップ接続する］をクリックし、［次へ］をクリックします。

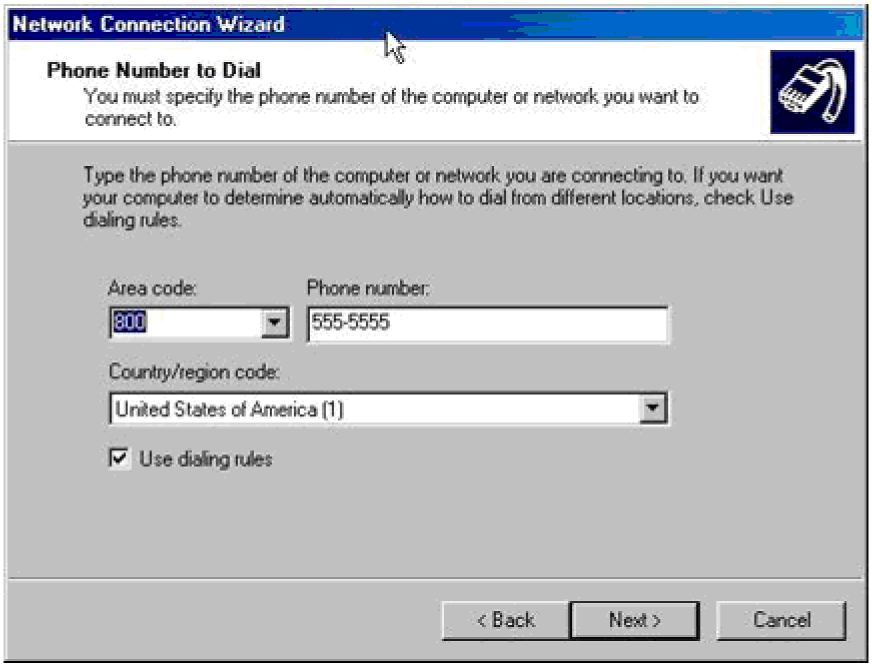


5. KSX II への接続に使用するモデムのチェックボックスをオンにし、［次へ］をクリックします。



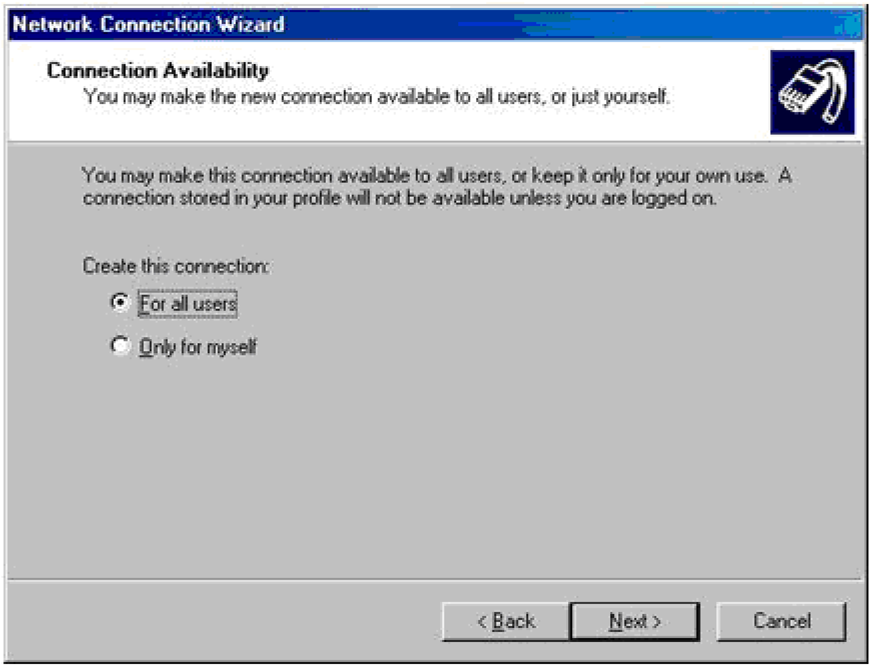
6. ダイヤル先の市外局番と電話番号を、該当のフィールドに入力します。

7. [国番号/地域番号] ドロップダウン矢印をクリックして、リストから国または地域を選択します。



8. [次へ] をクリックします。[接続の利用範囲] ダイアログ ボックスが表示されます。

9. [接続の利用範囲] ダイアログ ボックスで、[自分のみ] ラジオ ボタンをクリックします。



10. [次へ] をクリックします。ネットワーク接続が作成されました。
11. ダイヤルアップ接続の名前を入力します。
12. [完了] をクリックします。
13. [ダイヤル] をクリックしてリモート マシンに接続します。接続が正常に確立できたことを示すダイアログ ボックスが表示されます。

エラー メッセージが表示された場合は、Windows 2000® のダイヤルアップ ネットワークに関するヘルプを参照してください。

Windows Vista のダイヤルアップ ネットワーク設定

1. [スタート]、[ネットワーク] をクリックします。[ネットワーク] ウィンドウが開きます。
2. ウィンドウの上部で [ネットワークと共有センター] を選択します。[ネットワークと共有センター] ウィンドウが開きます。
3. [接続またはネットワークのセットアップ] を選択します。
4. [ダイヤルアップ接続のセットアップ] を選択します。[ダイヤルアップ接続のセットアップ] ダイアログが開きます。
5. ダイヤルアップ番号を入力します。
6. ユーザ名とパスワードを入力します。

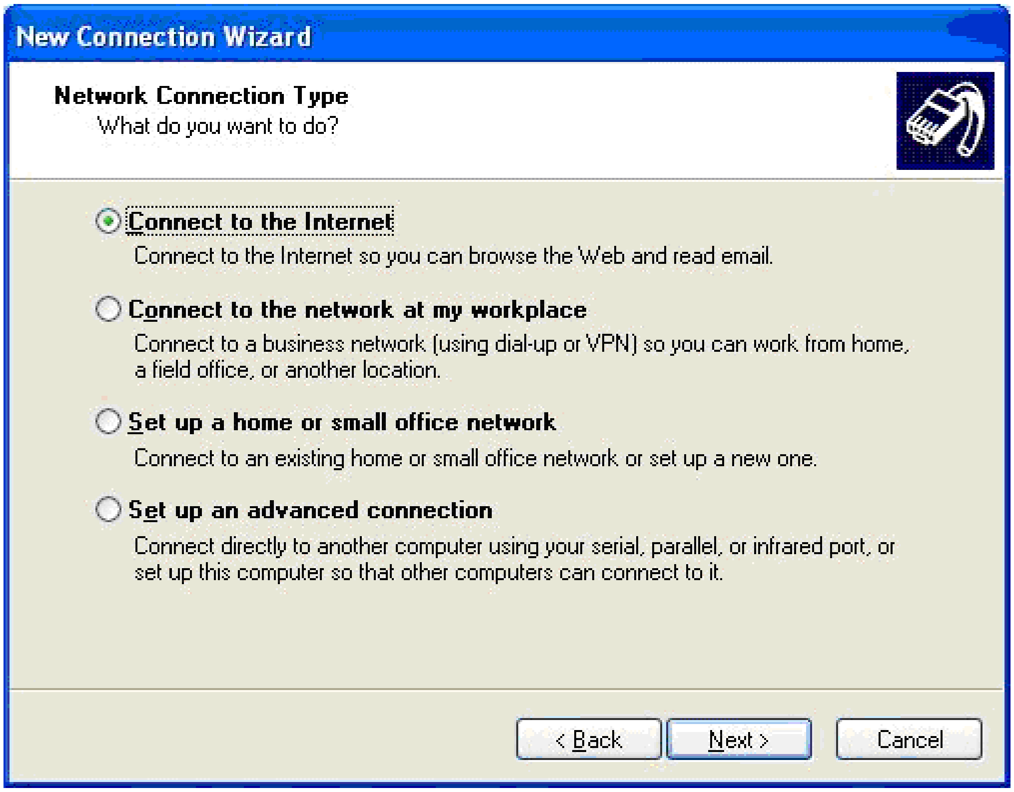
注: KSX II にアクセスするには、ユーザ名とパスワードに ¥(バックスラッシュ) を使用できません。

7. ［接続］をクリックします。

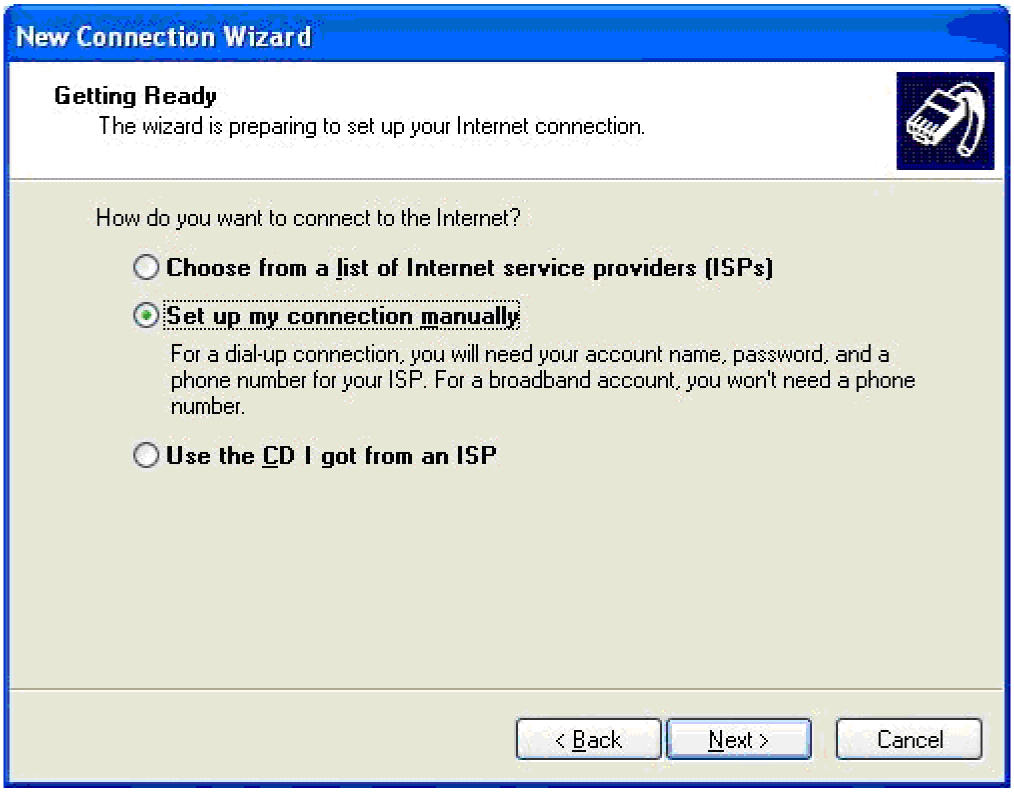
Windows XP のダイヤルアップ ネットワーク設定

1. ［スタート］、［すべてのプログラム］、［アクセサリ］、［通信］、［新しい接続ウィザード］を選択します。
2. ［次へ］をクリックして、［新しい接続ウィザード］ダイアログ ボックスの手順に従います。これからダイヤルアップ ネットワークのプロファイルを作成します。

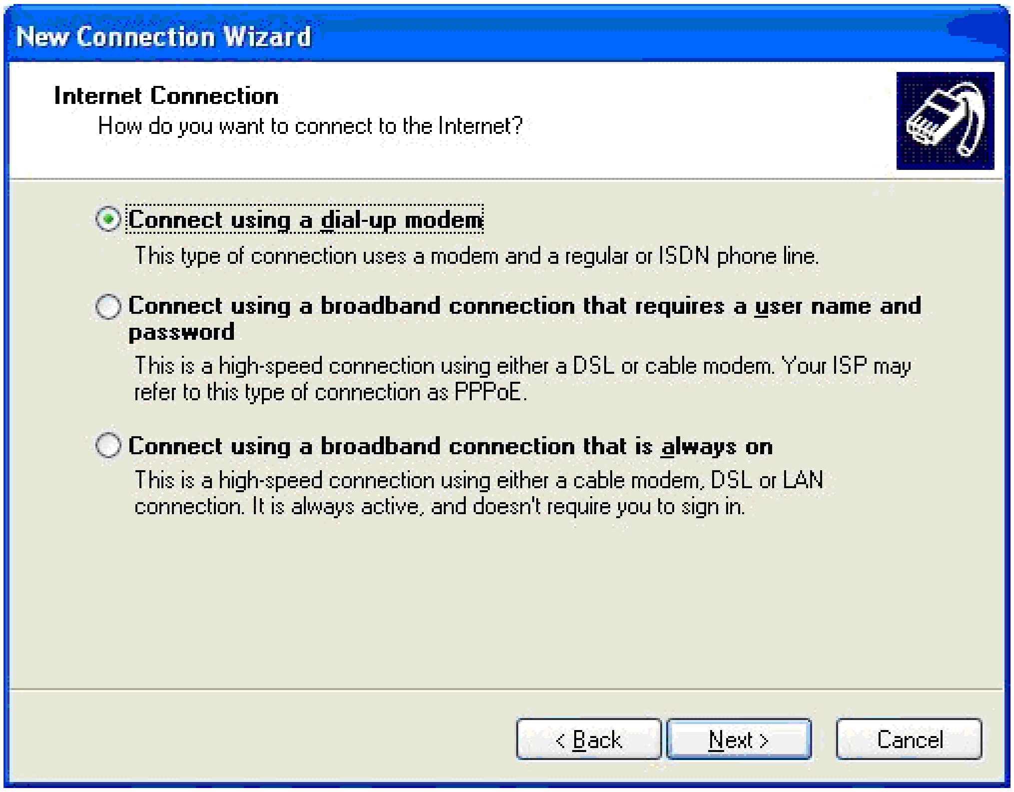
3. ［インターネットに接続する］ラジオ ボタンをクリックし、［次へ］をクリックします。



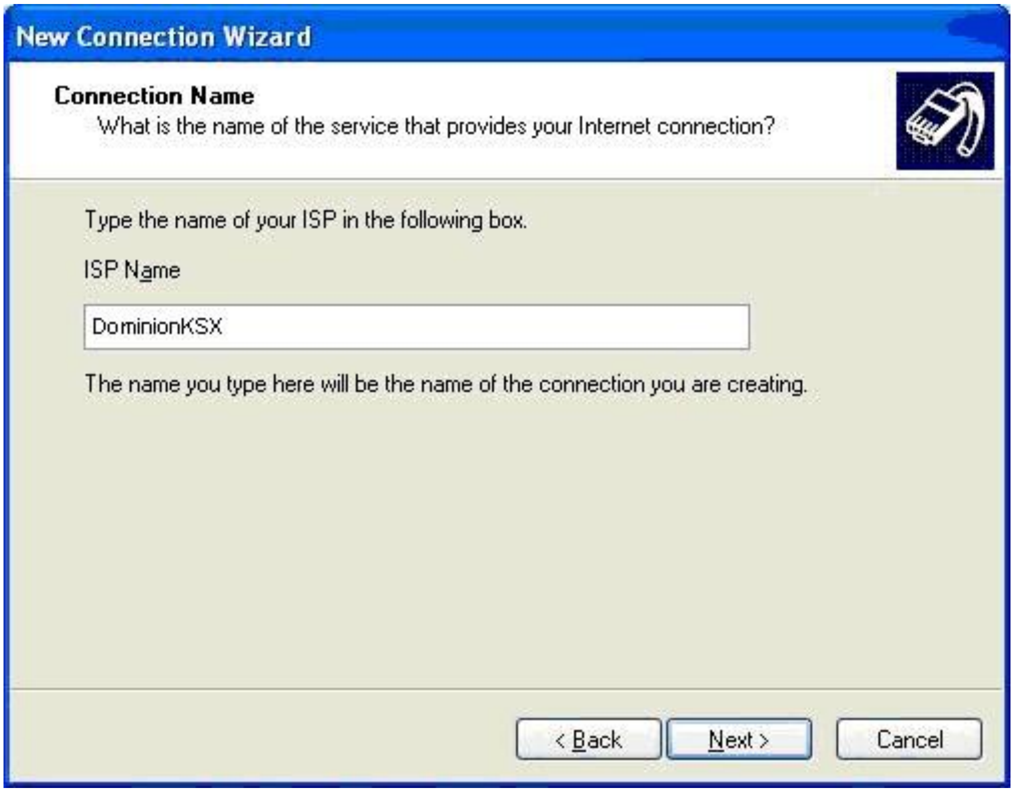
4. [接続を手動でセットアップする] ラジオ ボタンをクリックし、[次へ] をクリックします。



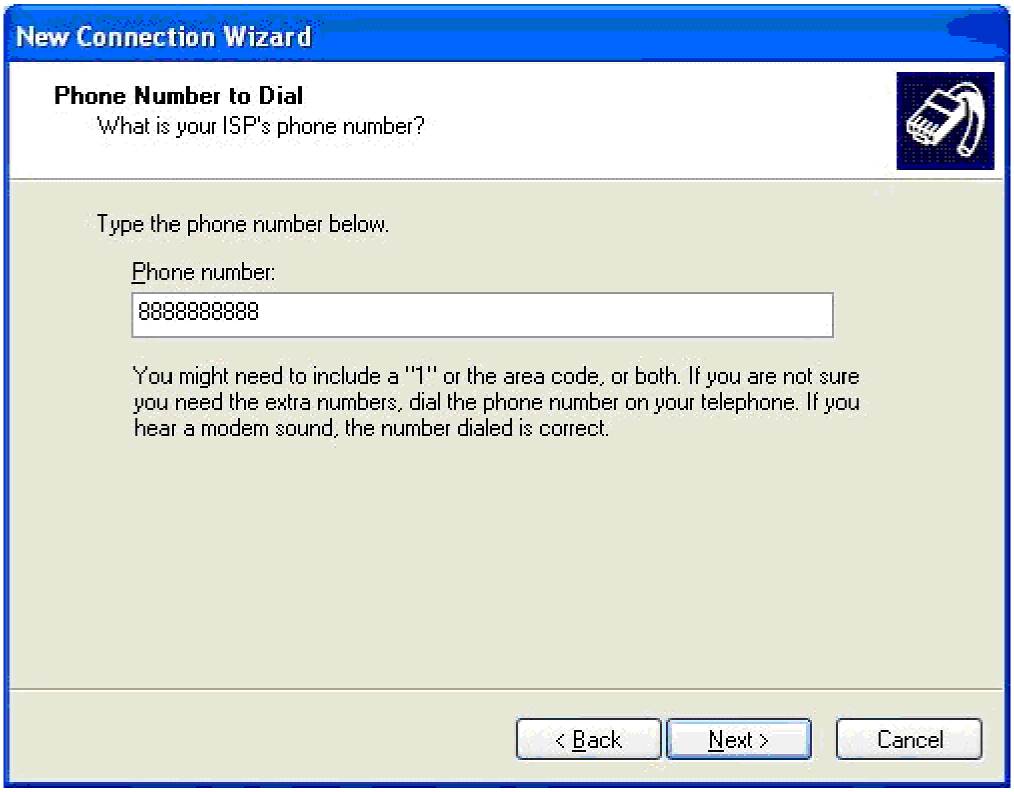
5. [ダイヤルアップ モデムを使用して接続する] ラジオ ボタンをクリックし、[次へ] をクリックします。



6. ［ISP 名］フィールドにこの接続を表す名前を入力し、［次へ］をクリックします。

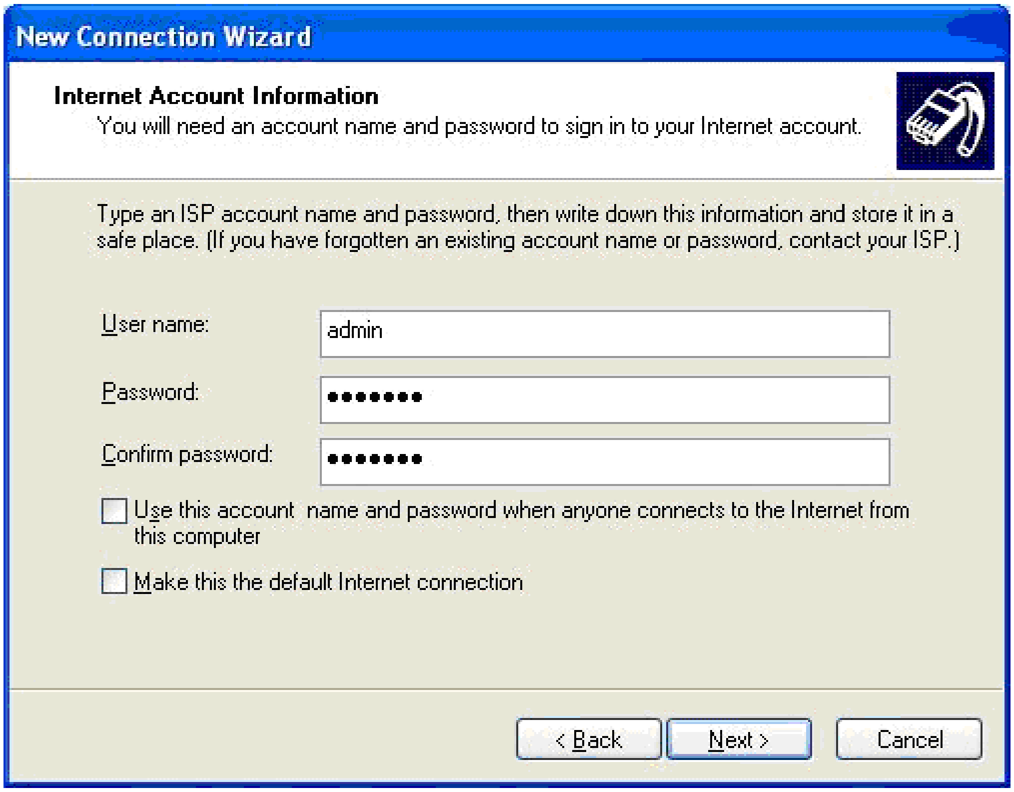


7. [電話番号] フィールドに接続先の電話番号を入力し、[次へ] をクリックします。



8. 自分の ISP 情報を入力します。ユーザ名とパスワードを該当するフィールドに入力し、確認のためにパスワードを再入力します。

9. フィールドの下にあるオプションで該当するチェックボックスをオンにし、［次へ］ をクリックします。



10. ［完了］をクリックします。
11. ［ダイヤル］をクリックしてリモート マシンに接続します。正常に接続されたことを示すダイアログが表示されます。エラーがあった場合は、Windows XP® のダイヤルアップ ネットワークに関するヘルプを参照してください。

注: KSX II に接続する最大モデム速度は 33,600 bps です。これは、Linux® のデフォルトの上限です。

Ap A　仕様

この章の内容

物理的仕様 297
サポートされているオペレーティング システム (クライアント) 298
サポートされているオペレーティング システムおよび CIM (KVM ターゲット サーバ) 299
サポートされているブラウザ 302
コンピュータ インタフェース モジュール (CIM) 302
サポートされている Paragon II CIMS および設定 303
サポートされている画面解像度 307
KSX II ローカル コンソールでサポートされる言語 308
使用される TCP ポートおよび UDP ポート 308
スマート カード リーダー 310
環境要件 313
緊急時の接続 314
電気的仕様 314
サポートされているリモート接続 315
KVM プロパティ 315
使用されるポート 315
サポートされているターゲット サーバとビデオ 317
シリアル デバイスの距離 317
ネットワーク速度の設定 318
接続 319
KSX II のシリアル RJ-45 ピン配列 320

物理的仕様

品目番号	品目説明	UPC コード	電力	重量	寸法 (幅 x 奥行き x 高さ)	出荷時重量	出荷時寸法 (幅 x 奥行き x 高さ)
KSX2144	4 KVM および 4 シリアル ポートの KSX II、複数ユーザ ネットワーク アクセス、ローカル ポート、仮想メディア	785813650054	100/240 V 50/60 Hz 0.6A 27 W	8.65 lbs	1.75 x 17.3 x 11.4 インチ	14.85 lbs	22 x 16.6 x 6.5 インチ
				3.9kg	44 x 439 x 290 mm	6.7 kg	559 x 422 x 165 mm

品目番号	品目説明	UPC コード	電力	重量	寸法 (幅 x 奥行き x 高さ)	出荷時重量	出荷時寸法 (幅 x 奥行き x 高さ)
KSX2188	8 KVM および 8 シリアル ポートの KSX II、複数ユーザ ネットワーク アクセス、ローカル ポート、仮想メディア	785813650047	100/240 V 50/60 Hz 0.6A 27 W	8.65 lbs	1.75 x 17.3 x 11.4 インチ	14.85 lbs	22 x 16.6 x 6.5 インチ
				3.9kg	44 x 439 x 290 mm	6.7 kg	559 x 422 x 165 mm

サポートされているオペレーティング システム (クライアント)

Virtual KVM Client (VKC) および Multi-Platform Client (MPC) でサポートされているオペレーティング システム (OS) は、次のとおりです。

クライアント オペレーティング システム	クライアントで仮想メディア (VM) がサポートされているか
Windows 7®	あり
Windows XP®	あり
Windows 2008®	あり
Windows Vista®	あり
Windows 2000® SP4 Server	あり
Windows 2003® Server	あり
Windows 2008® Server	あり
Red Hat® Desktop 5.0	あり
Red Hat Desktop 4.0	あり
openSUSE 10、11	あり
Fedora® 13 および 14	あり
Mac® OS	あり
Solaris™	なし
Linux®	あり (ISO イメージの場合)

Java Runtime Environment (JRE™) プラグインは、32 ビット版および 64 ビット版 Windows® で使用できます。MPC および VKC は、32 ビット版ブラウザ、64 ビット版 Internet Explorer 7、または 64 ビット版 Internet Explorer 8 からのみ起動できます。

次の表に、Java™ 32 ビットおよび 64 ビット Windows におけるソフトウェア要件を示します。

モード	オペレーティング システム	ブラウザ
Windows x64 32 ビット モード	Windows XP®	• Internet Explorer® 6.0 SP1 以降、IE 7、IE 8 • Firefox® 1.06 ～ 4 以降
	Windows Server 2003®	• Internet Explorer 6.0 SP1 以降、IE 7、IE 8 • Firefox 1.06 ～ 3
	Windows Vista®	• Internet Explorer 7.0 または 8.0
	Windows 7®	• Internet Explorer 9.0 • Firefox 1.06 ～ 4 以降
Windows x64 64 ビット モード	Windows XP	64 ビット OS 対応の 32 ビット版ブラウザ • Internet Explorer 6.0 SP1 以降、7.0、または 8.0 • Firefox 1.06 ～ 4 以降 64 ビット OS 対応の 64 ビット版ブラウザ • Internet Explorer 7.0 または 8.0
	Windows XP Professional®	
	Windows XP Tablet®	
	Windows Vista	
	Windows Server 2003	
	Windows Server 2008	
	Windows 7	

サポートされているオペレーティング システムおよび CIM (KVM ターゲット サーバ)

新しい D2CIM に加え、Dominion CIM がサポートされています。次の表に、サポートされているターゲット サーバ オペレーティング システム、CIM、仮想メディア、およびマウス モードを示します。

注: D2CIM-VUSB は、Sun™ (Solaris™) ターゲット サーバではサポートされていません。

サポートされる Dominion CIM & D2CIM	OS およびシリアル デバイス	仮想メディア	ずれないマウス モード	インテリジェント マウス モード	標準マウス モード
• DCIM-PS2 • DCIM-PS2 • DCIM-USB • DCIM-USB G2	• Windows XP® オペレーティング システム • Windows 2000® オペレーティング システム • Windows Server 2000® • Windows Server 2003® • Windows Vista® オペレーティング システム			✓	✓
• D2CIM-VUSB	• Windows XP® オペレーティング システム • Windows 2000® オペレーティング システム • Windows Server 2000® • Windows Server 2003® • Windows Vista® オペレーティング システム	✓	✓	✓	✓

ターゲット サーバ	サポートされている CIM		マウス モード			
	Dominion DCIM	D2CIM	[VM] (VM)	AM	IM	SM
Windows XP オペレーティング システム Windows 2000 オペレーティング システム Windows Server 2000® Windows Server 2003® Windows Vista オペレーティング システム			✓	✓	✓	✓

ターゲット サーバ	サポートされている CIM		マウス モード			
Red Hat® Enterprise Workstation 3.0、4.0、および 5.0	DCIM-PS2 DCIM-USB DCIM-USB G2	D2CIM-VUSB (Red Hat Enterprise Workstation 3.0 を除く)	✓		✓	✓
SUSE Linux Professional 9.2 および 10	DCIM-PS2 DCIM-USB DCIM-USB G2	D2CIM-VUSB	✓			✓
Fedora® Core 3® 以降	DCIM-PS2 DCIM-USB DCIM-USB G2	D2CIM-VUSB	✓			✓
Mac OS	DCIM-USB DCIM-USB G2	D2CIM-VUSB	✓	✓		
Dominion KSX II でサポートされているすべての Solaris OS	DCIM-SUN DCIM-SUSB DCIM-USB G2				✓	✓
IBM® AIX®	DCIM-USB DCIM-USB G2 DCIM-PS2					✓
HP UX®	DCIM-USB DCIM-USB G2 DCIM-PS2					✓
シリアル デバイス	P2CIM-SER				✓	

凡例:

- VM – 仮想メディア (D2CIM-VUSB のみ)
- AM:Absolute Mouse Synchronization (D2CIM-VUSB のみ)
- IM:インテリジェント マウス モード
- SM:標準マウス モード
- ✓: サポートされています。

DCIM-USB G2 の背面には小さいスライド型スイッチがあります。PC ベースの KVM ターゲット サーバを USB で接続する場合は、このスイッチを P にします。Sun の KVM ターゲット サーバを USB で接続する場合は、このスイッチを S にします。
変更後のスイッチ位置が有効になるのは、CIM に給電し直した後です。CIM に給電し直すには、ターゲット サーバから USB コネクタをいったん取り外し、数秒経ってから再度取り付けます。

サポートされているブラウザ

KSX II でサポートされているブラウザは、次のとおりです。

- Internet Explorer® 7 ～ 9
- Firefox® 4 以降
- Safari® 3 以降

コンピュータ インタフェース モジュール (CIM)

品目番号	品目説明	UPC コード	重量	寸法 (幅 x 奥行き x 高さ)	出荷時重量	出荷時寸法 (幅 x 奥行き x 高さ)
D2CIM-VUSB	KSX II 用 CIM、[USB ポート、仮想メディア機能]	785813332004	0.2 lbs	1.3 x 3.0 x 0.6 インチ	0.2 lbs	7.2 x 9 x 0.6 インチ
DCIM-SUN	KSX II 用 CIM、[Sun ポート、HD15 ビデオ]	785813338549	0.2 lbs	1.3 x 3.0 x 0.6 インチ	0.2 lbs	7.2 x 9 x 0.6 インチ

サポートされている Paragon II CIMS および設定

KSX II では P2CIM-APS2DUAL CIM および P2CIM-AUSBDUAL CIM がサポートされています。これらの CIM を使用した場合、RJ45 で 2 台の異なる KVM スイッチに接続できます。

これらの CIM がサポートされているので、KVM スイッチのいずれかに障害が発生した場合に備えて、ターゲットにアクセスするための 2 つ目の経路を確保できます。

Paragon CIM	サポートされるもの	サポートされないもの
P2CIM-APS2DUAL	• IBM® PS/2 型のキーボード ポートとマウス ポートを備えたサーバ • 自動スキュー補正 (CIM が Paragon II に接続されているが、KSX II に接続されていない場合) • インテリジェント マウス モード • 標準マウス モード	• 仮想メディア • スマート カード • ずれないマウス モード • ブレード シャーシとの併用 • KVM のカスケード接続構成
P2CIM-AUSBDUAL	• USB 型または Sun™ USB 型のキーボード ポートとマウス ポートを備えたサーバ • 自動スキュー補正 (CIM が Paragon II に接続されているが、KSX II に接続されていない場合) • インテリジェント マウス モード • 標準マウス モード	• 仮想メディア • スマート カード • ずれないマウス モード • ブレード シャーシとの併用 • KVM のカスケード接続構成

KSX II - KSX II 構成の Paragon CIM に関するガイドライン

KSX II – KSX II 構成で Paragon CIM を使用する場合は、次に示すシステム構成ガイドラインに従ってください。

同時アクセス

両方の KSX II KVM スイッチで、ターゲットへの同時アクセスに対して同じポリシーを設定する必要があります。つまり、どちらも [PC-Share] (PC 共有) にするか、どちらも [Private] (プライベート) に設定します。

ターゲットへのプライベート アクセスが必要な場合は、どちらの KVM スイッチもそれに応じて構成する必要があります。

- [Security] (セキュリティ)、[Security Settings] (セキュリティ設定)、[Encryption & Share] (暗号化および共有) を選択し、[PC Share Mode] (PC 共有モード) を [Private] (プライベート) に設定します。

これにより、すべてのユーザ グループおよびすべてのターゲットにおいて、ターゲットへの同時アクセスはできなくなります。

KSX II では、ターゲットへの同時アクセスをより高い粒度で、ユーザ グループ単位で制御できます。これは、ユーザ グループの PC 共有権限を設定することで行われます。ただし、これが適用されるのは KSX II の範囲内のみです。P2CIM-APS2DUAL または P2CIM-AUSBDUAL を KSX II と組み合わせて使用する際にプライバシーを保証する必要がある場合、ユーザ グループに対する PC 共有権限を使用しないでください。

CIM 名の更新

P2CIM-APS2 および P2CIM-AUSB の名前は CIM のメモリに保持されています。メモリ上には、Paragon CIM の名前 (最大 12 文字) を保持するための領域と、KSX II の名前 (最大 32 文字) を保持するための領域の、2 つの領域があります。

Paragon CIM を KSX II に初めて接続したとき、CIM の名前がメモリから取得され、KSX II によって使用される CIM のメモリ領域に書き込まれます。続いて、KSX II から、KSX II によって使用されるメモリ領域に対して、CIM 名の照会または更新が行われます。KSX II から、Paragon II によって使用されるメモリ領域に対して更新が行われることはありません。

一方の KSX II によって CIM 名が更新されると、もう一方の KSX II がそのターゲットへの接続を試みるときに、更新後の CIM 名が検出および取得されます。そのときまで、この CIM 名がもう一方の KSX II 上で更新されることはありません。

ポートのステータスと可用性

ポートのステータスは、KSX II の [Port Access] (ポート アクセス) ページに [Up] (稼動) または [Down] (非稼動) として表示されます。このステータスは最新の情報に更新され、CIM の電源が入っていて KSX II のポートに接続されているかどうかが示されます。

ポートの可用性は、KSX II の [Port Access] (ポート アクセス) ページに [Idle] (アイドル)、[Busy] (ビジー)、または [Connected] (接続) として表示されます。この可用性情報は、同じ KSX II から起動されたターゲットの稼動状況を反映するように更新されます。

もう一方の KSX II からそのターゲットに接続している場合は、この KSX II から接続が試みられたときに可用性が検査されます。KSX II に対して設定されている PC 共有ポリシーに基づいて、アクセスが拒否または許可されます。そのときまで、この可用性情報がもう一方の KSX II 上で更新されることはありません。

ターゲットがビジーであるためにアクセスが拒否された場合、通知が表示されます。

CC-SG との連係動作

CC-SG から起動される処理は、管理対象 KSX II から通知されるステータス、可用性情報、および CIM 名に基づいて決まります。ターゲットが 2 台の管理対象 KSX II に接続されており、これらの KSX II が CC-SG に追加されている場合、ノードが 2 つ作成されます。各ノードには固有の oob-kvm インタフェースが関連付けられます。各 KSX II の oob-kvm インタフェースで、単一のノードを設定することもできます。

KSX II がプライベート モードに設定されている場合、2 つ目の接続が試みられると、"接続できず、アクセスが拒否された" という内容のメッセージがユーザに表示されます。

CC-SG の [Port Profile] (ポート プロファイル) ペインでポート名を変更すると、変更後の名前が管理対象 KSX II にプッシュ送信されます。もう一方の KSX II の対応するポート名は、そのもう一方の oob-kvm インタフェース経由でターゲットへの接続が試みられるまで、CC-SG 内で更新されません。

KSX II - Paragon II 構成に関するガイドライン

P2CIM-APS2DUAL または P2CIM-AUSBDUAL を使用して KSX II と Paragon II を接続できます。

同時アクセス

KSX II と Paragon II の両方で、ターゲットへの同時アクセスに関して同じポリシーを設定してください。

Paragon II の動作モード	モードの説明	サポート
プライベート	特定のチャネル ポートに接続されているサーバなどのデバイスに、同時に 1 人のユーザだけが排他アクセスできます。	サポートされています。 Paragon II と KSX II の両方を [Private] (プライベート) に設定する必要があります。プライベート設定は、ユーザグループごとではなく KSX

Paragon II の動作モード	**モードの説明**	**サポート**
		II に対して適用されます。 Paragon II では、赤は "ビジー"、緑は "使用可能" を意味します。
PC 共有	特定のチャネル ポートに接続されているサーバなどのデバイスを、複数のユーザが選択して制御することができます。ただし、キーボードとマウスを制御できるユーザは同時に 1 人だけです。	サポートされています。 ただし、Paragon II で設定される PC 共有アイドル タイムアウトはサポートされていません。両方のユーザが、キーボードとマウスを同時に制御できます。 Paragon II では、緑は "使用可能" を意味します。このことは、別のユーザが既にターゲットにアクセスしている場合にも当てはまります。
パブリック表示	一方のユーザが、特定のチャネル ポートに接続されているサーバなどのデバイスにアクセスしている間、もう一方のユーザは、そのチャネル ポートを選択し、そのデバイスからのビデオ出力を表示することができます。ただし、キーボードとマウスを制御できるのは、最初にアクセスしたユーザだけです。両方のユーザが切断するか、またはキーボードとマウスを取り外すと、この状態が解消されます。	サポートされていません。 Paragon II と KSX II を CIM で接続している場合、このモードは使用できません。 Paragon II では、黄色はパブリック表示モードを意味します。

CIM 名の更新

- Paragon II から更新された CIM 名は、Paragon の命名規則に対応する CIM メモリ領域に保持され、この領域から取得されます。
- KSX II から更新された CIM 名は、KSX II の命名規則に対応する CIM メモリ領域に保持され、この領域から取得されます。
- CIM 名が更新されても、Paragon II と KSX II の間で互いに反映されることはありません。

サポートされている画面解像度

各ターゲット サーバの画面解像度とリフレッシュ レートが KSX II でサポートされているかどうか、および、映像信号がノンインタレース方式であるかどうかを確認してください。

画面解像度とケーブル長は、マウスを同期させるうえで重要な要素です。

KSX II でサポートされている画面解像度は次のとおりです。

解像度	
640x350、70Hz	1024x768、85Hz
640x350、85Hz	1024x768、75Hz
640x400、56Hz	1024x768、90Hz
640x400、84Hz	1024x768、100Hz
640x400、85Hz	1152x864、60Hz
640x480、60Hz	1152x864、70Hz
640x480、66.6Hz	1152x864、75Hz
640x480、72Hz	1152x864、85Hz
640x480、75Hz	1152x870、75.1Hz
640x480、85Hz	1152x900、66Hz
720x400、70Hz	1152x900、76Hz
720x400、84Hz	1280x720、60Hz
720x400、85Hz	1280x960、60Hz
800x600、56Hz	1280x960、85Hz
800x600、60Hz	1280x1024、60Hz
800x600、70Hz	1280x1024、75Hz
800x600、72Hz	1280x1024、85Hz

解像度	
800x600、75Hz	1360x768、60Hz
800x600、85Hz	1366x768、60Hz
800x600、90Hz	1368x768、60Hz
800x600、100Hz	1400x1050、60Hz
832x624、75.1Hz	1440x900、60Hz
1024x768、60Hz	1600 x 1200、60Hz
1024x768、70Hz	1680x1050、60Hz
1024x768、72Hz	1920x1080、60Hz

注: 映像信号が Composite Sync 方式または Sync on Green 方式である場合は、アダプタを増設する必要があります。

注:一部の解像度は、デフォルトでは使用できない可能性があります。解像度が表示されない場合は、まずモニタを接続し、モニタを取り外してから CIM を接続します。

注:解像度 1440x900 および 1680x1050 がターゲット サーバのグラフィック アダプタ カードでサポートされているにもかかわらず表示されない場合は、DDC-1440 または DDC-1680 アダプタが必要である可能性があります。

KSX II ローカル コンソールでサポートされる言語

KSX II ローカル コンソールは、次の言語のキーボードをサポートしています。英語 (アメリカ)、英語 (イギリス)、ドイツ語、フランス語、日本語、韓国語、簡体字中国語、繁体字中国語。

注: 中国語、日本語、および韓国語のキーボードについては、表示のみに使用できます。現時点での KSX II ローカル コンソール機能では、ローカル言語の入力はサポートされていません。

使用される TCP ポートおよび UDP ポート

ポート	説明
HTTP、ポート 80	このポートは、必要に応じて設定できます。詳細については、「***HTTP ポートおよび HTTPS ポートの設定*** 『***154***p. 』」を参照してください。セキュリティを確保するため、デフォルトでは、KSX II によって HTTP (ポート 80) で受信された要求は、すべて HTTPS に自動変換されます。要求はポート 80 で受け付けられるので、ユーザはブラウザのアドレスボックスに明示的に「https://」と入力する必要はありません。また、セキュリティも確保されます。
HTTP、ポート 443	このポートは、必要に応じて設定できます。詳細については、「***HTTP ポートおよび HTTPS ポートの設定*** 『***154***p. 』」を参照してください。デフォルトでは、このポートはさまざまな目的で使用されます。たとえば、クライアントから HTML で Web サーバにアクセスする場合、クライアント ソフトウェア (MPC/VKC) をクライアントにダウンロードする場合、KVM データと仮想メディア データをクライアントに転送する場合などです。
KSX II (Raritan KVM-over-IP) プロトコル、ポート 5000 (変更可)	このポートは、他の Dominion デバイスの検出、および Raritan デバイスと各種システム (CC-SG 管理で利用可能なデバイス向けの CC-SG など) との間の通信に使用されます。このポートはデフォルトで 5000 に設定されていますが、別の TCP ポートに変更することもできます。この設定を変更する手順については、「***ネットワーク設定*** 『***147***p. 』」を参照してください。
SNTP (時刻サーバ)、UDP ポート 123 (変更可)	KSX II の内部クロックを中央の時刻サーバと同期させることができます。この機能を利用するには UDP ポート 123 (SNTP 用の標準ポート) を使用する必要がありますが、別のポートに変更することもできます。**(オプション)**
LDAP/LDAPS、ポート 389 または 636 (変更可)	LDAP/LDAPS プロトコルを使用してユーザをリモート認証するように KSX II が設定されている場合、デフォルトでポート 389 または 636 が使用されます。ただし、別のポートに変更することもできます。**(オプション)**
RADIUS、ポート 1812 (変更可)	RADIUS プロトコルを使用してユーザをリモート認証するように KSX II が設定されている場合、デフォルトでポート 1812 が使用されます。ただし、別のポートに変更することもできます。**(オプション)**
設定可能なポート 1813 を使用する RADIUS アカウンティング	RADIUS プロトコルを使用してユーザをリモート認証するように KSX II が設定されており、かつ、イベントのログ記録に RADIUS アカウンティングが使用されている場合、ログ通知の転送にデフォルトでポート 1813 が使用されます。ただし、別のポートに変更することもできます。
SYSLOG、UDP ポート 514 (変更可)	メッセージを Syslog サーバに送信するように KSX II が設定されている場合、通信にデフォルトでこのポートが使用されます。ただし、別のポートに変更することもできます。

SNMP、デフォルトの UDP ポート	送受信の読み取り/書き込み SNMP アクセスにはポート 161 が使用されます。SNMP トラップの送信トラフィックにはポート 162 が使用されます。**(オプション)**
TCP ポート 22	ポート 22 は、KSX II のコマンド ライン インタフェース (CLI) を利用する際に使用されます (お客様が Raritan のテクニカル サポート部門と協力して作業する場合)。

スマート カード リーダー

サポートされているスマート カード リーダーとサポートされていないスマート カード リーダー

外付けの USB スマート カード リーダーがサポートされています。

サポートされているスマート カード リーダー

タイプ	ベンダ	[Model] (モデル)	検証
USB	SCM Microsystems	SCR331	ローカルおよびリモートで検証済み
USB	ActivIdentity®	ActivIdentity USB Reader v2.0	ローカルおよびリモートで検証済み
USB	ActivIdentity	ActivIdentity USB Reader v3.0	ローカルおよびリモートで検証済み
USB	Gemalto®	GemPC USB-SW	ローカルおよびリモートで検証済み
USB キーボード/カード リーダーの組み合わせ	Dell®	USB Smart Card Reader Keyboard	ローカルおよびリモートで検証済み
USB キーボード/カード リーダーの組み合わせ	Cherry GmbH	G83-6744 SmartBoard	ローカルおよびリモートで検証済み
SIM サイズのカードに対応した USB リーダー	Omnikey	6121	ローカルおよびリモートで検証済み
統合型 (Dell Latitude D620)	O2Micro	OZ776	リモートのみ
PCMCIA	ActivIdentity	ActivIdentity PCMCIA Reader	リモートのみ

タイプ	ベンダ	[Model] (モデル)	検証
USB	SCM Microsystems	SCR331	ローカルおよびリモートで検証済み
PCMCIA	SCM Microsystems	SCR243	リモートのみ

注: SCM Microsystems の SCR331 スマート カード リーダーでは、SCM Microsystems のファームウェア v5.25 を使用する必要があります。

サポートされていないスマート カード リーダー

この表は、Raritan がテストし、Raritan デバイスでは動作しないことが判明しているリーダーの一覧です。したがって、これらのリーダーはサポートされていません。サポートされているスマート カード リーダーの表にもサポートされていないスマート カード リーダーの表にもないスマート カード リーダーについては、デバイスでの動作を保証できません。

タイプ	ベンダ	[Model] (モデル)	注意
USB キーボード/カード リーダーの組み合わせ	HP®	ED707A	インタラプト エンドポイントなし => Microsoft® ドライバとの互換性なし
USB キーボード/カード リーダーの組み合わせ	SCM Microsystems	SCR338	独自のカード リーダー実装 (CCID 非準拠)
USB トークン	Aladdin®	eToken PRO™	独自の実装

スマート カードの最小システム要件

ローカル ポートの要件

KSX II へのローカル ポート接続の相互運用性の基本要件は、以下のとおりです。

- ローカルに接続されたすべてのデバイス (スマート カード リーダーまたはトークン) は、USB CCID に準拠している必要があります。

ターゲット サーバの要件

スマート カード リーダーを使用する場合、ターゲット サーバにおける相互運用性の基本要件は以下のとおりです。

- IFD (スマート カード リーダー) Handler は、標準の USB CCID デバイス ドライバ (汎用の Microsoft® USG CCID ドライバに相当) である必要があります。
- デジタル CIM または D2CIM-DVUSB (デュアル VM CIM) が必要であり、そのファームウェア バージョンは 3A6E 以降である必要があります。
- ブレード シャーシのサーバ接続 (ブレードごとに CIM を使用) がサポートされます。
- ブレード シャーシのサーバ接続 (シャーシごとに CIM を使用) は、自動検出が有効になっている IBM® BladeCenter® モデル H および F でのみサポートされます。

Windows XP ターゲット

Windows XP® ターゲットでは、KSX II でスマート カードを使用するために Windows XP SP3 が実行されている必要があります。ターゲット サーバ上の Windows XP 共有で .NET 3.5 を実行している場合、SP1 を適用する必要があります。

Linux ターゲット

Linux® ターゲットを使用している場合、Raritan デバイスでスマート カード リーダーを使用するには、以下の要件を満たす必要があります。

- CCID の要件

  Linux ターゲットで Raritan D2CIM-DVUSB VM/CCID がスマート カード リーダーとして認識されない場合は、CCID ドライバのバージョンを 1.3.8 以上に更新し、ドライバ設定ファイル (Info.plist) を更新する必要があります。

オペレーティング システム	CCID の要件
RHEL 5	ccid-1.3.8-1.el5
SuSE 11	pcsc-ccid-1.3.8-3.12
Fedora® Core 10	ccid-1.3.8-1.fc10.i386

リモート クライアントの要件

リモート クライアントにおける相互運用性の基本要件は、以下のとおりです。

- IFD (スマート カード リーダー) Handler は、PC/SC 準拠のデバイス ドライバである必要があります。
- ICC (スマート カード) Resource Manager が使用可能で、PC/SC 準拠である必要があります。
- スマート カード API を含む JRE™ 1.6.x が Raritan クライアント アプリケーションで使用可能である必要があります。

Linux クライアント

Linux® クライアントを使用している場合、Raritan デバイスでスマート カード リーダーを使用するには、以下の要件を満たす必要があります。

注: ターゲットへの 1 つ以上の KVM セッションがアクティブになっている場合、スマート カードを挿入すると、クライアントへのユーザ ログインに時間がかかることがあります。これらのターゲットへのログイン プロセスも進行中です。

- PC/SC の要件

オペレーティング システム	必要な PC/SC
RHEL 5	pcsc-lite-1.4.4-0.1.el5
SuSE 11	pcsc-lite-1.4.102-1.24
Fedora® Core 10	pcsc-lite-1.4.102.3.fc10.i386

- Java™ ライブラリ リンクの作成

  RHEL 4、RHEL 5、および FC 10 のアップグレード後、libpcsclite.so へのソフト リンクを作成する必要があります。たとえば、パッケージのインストールによってライブラリが /usr/lib または /user/local/lib に配置される場合、「ln -s /usr/lib/libpcsclite.so.1 /usr/lib/libpcsclite.so」と入力します。

- PC/SC デーモン

  pcsc デーモン (フレームワークのリソース マネージャ) を再起動する場合は、ブラウザと MPC も再起動します。

環境要件

作動時	
温度	0 ℃～ 40 ℃

作動時	
湿度	20 ～ 85%（相対湿度）
標高	なし
振動	5-55-5 HZ、0.38 mm、1 サイクル 1 分、 軸（X、Y、Z）ごとに 30 分
衝撃	なし
非作動時	
温度	0 ～ 50 ℃
湿度	10 ～ 90%（相対湿度）
標高	なし
振動	5-55-5 HZ、0.38 mm、1 サイクル 1 分、 軸（X、Y、Z）ごとに 30 分
衝撃	なし

緊急時の接続

接続	説明
オプションのモデム接続	ネットワークに障害が発生した場合の緊急リモートアクセス用です。
ターゲット デバイスの接続	簡略化された RJ45 ベース CAT 5 ケーブルによる方法で、シリアル ポート アダプタは Raritan より提供されます。
ローカル アクセス	「緊急用カート」アプリケーション向けのローカル アクセスです。

KSX II を一般的なベンダ/モデルの組み合わせに接続するのに必要な KSX II ハードウェア（アダプタおよびケーブル）の一覧は、「*接続*『*319*p. 』」を参照してください。

電気的仕様

パラメータ	値
入力	

パラメータ		値
	定格周波数	50/60 Hz
	定格電圧範囲	100/240 VAC
	最大電流 AC RMS	最大 0.6 A
	AC 動作範囲	100 ～ 240 VAC (+-10%)、47 ～ 63 Hz

サポートされているリモート接続

リモート接続	詳細情報
ネットワーク	10BASE-T、100BASE-T、および 1000BASE-T (Gigabit) Ethernet
プロトコル	TCP/IP、UDP、SNTP、HTTP、HTTPS、RADIUS、LDAP/LDAPS

KVM プロパティ

- キーボード - USB
- マウス - USB
- ビデオ - VGA

使用されるポート

ポート	説明
HTTP、ポート 80	セキュリティを確保するため、KSX II によって HTTP (ポート 80) で受信される要求は、すべて HTTPS に自動的に転送されます。要求はポート 80 で受け付けられるので、ユーザはブラウザのアドレス ボックスに明示的に「https://」と入力する必要はありません。また、セキュリティも確保されます。
HTTP、ポート 443	このポートは、KSX II デバイスからユーザのデスクトップ上の KVM クライアントに対し、KVM-over-IP 通信を実際に行う際に使用されます。この設定は変更できません。
KSX II (Raritan	このポートは、他の KX デバイスの検出、およ

ポート	説明
KVM-over-IP) プロトコル、ポート 5000 (変更可)	び、Raritan デバイスと各種システム (例: CommandCenter Secure Gateway (CC-SG)) との間の通信に使用されます。デフォルトではポート 5000 に設定されていますが、80 と 443 以外であれば、どの TCP ポートを使用するよう設定してもかまいません。この設定方法については、「*[Network Settings] (ネットワーク設定)*『*147*p. の"*ネットワーク設定*"参照 』」を参照してください。
設定可能な UDP ポート 123 を使用する SNTP (時刻サーバ) **(オプション)**	KSX II の内部クロックを中央の時刻サーバと同期させることができます。この機能を利用するには UDP ポート 123 (SNTP 用の標準ポート) を使用する必要がありますが、別のポートに変更することもできます。
設定可能なポート 389 および 636 を使用する LDAP/LDAPS **(オプション)**	LDAP/LDAPS プロトコルを使用してユーザをリモート認証するように KSX II が設定されている場合、デフォルトでポート 389 または 636 が使用されます。ただし、別のポートに変更することもできます。
設定可能なポート 1812 を使用する RADIUS **(オプション)**	RADIUS プロトコルを使用してユーザをリモート認証するように KSX II が設定されている場合、デフォルトでポート 1812 または 1813 が使用されます。ただし、別のポートに変更することもできます。
設定可能なポート 1813 を使用する RADIUS アカウンティング	RADIUS プロトコルを使用してユーザをリモート認証するように KSX II が設定されており、かつ､イベントのログ記録に RADIUS アカウンティングが使用されている場合、ログ通知の転送にデフォルトでポート 1813 が使用されます。ただし、別のポートに変更することもできます。
SYSLOG、UDP ポート 514 (変更可)	メッセージを Syslog サーバに送信するように KSX II が設定されている場合、通信にデフォルトでこのポートが使用されます。ただし、別のポートに変更することもできます。
SNMP デフォルト UDP ポート **(オプション)**	送受信の読み取り/書き込み SNMP アクセスにはポート 161 が使用されます。SNMP トラップの送信トラフィックにはポート 162 が使用されます。

ポート	説明
SSH	SSH (Secure Shell) ポートは設定できます。デフォルトはポート 22 です。
Telnet	Telnet ポートは設定できますが、お勧めしません。デフォルト ポートは 23 です。

サポートされているターゲット サーバとビデオ

サポートされる最大接続距離は、さまざまな要素によって決まります。たとえば、Cat5 ケーブルのタイプと品質、サーバのタイプと製造元、ビデオ ドライバとモニタ、環境条件、ユーザの要求レベルなどに左右されます。

次の表に、各種の画面解像度とリフレッシュ レートにおける最大接続距離を示します。

画面解像度	リフレッシュ レート	最大接続距離
1920 x 1080	60	15 m (50 フィート)
1600 x 1200	60	15 m (50 フィート)
1280 x 1024	60	30 m (100 フィート)
1024 x 768	60	45 m (150 フィート)

注: サーバの製造メーカーやタイプ、OS のバージョン、ビデオ ドライバなどは多種多様であるうえ、ビデオ品質にはユーザーの主観が反映されるため、Raritan ではあらゆる環境でのすべての距離におけるパフォーマンスを保証することはできません。

KSX II でサポートされている画面解像度については、「***サポートされている画面解像度*** 『*307*p. 』」を参照してください。

シリアル デバイスの距離

シリアル デバイスの標準的な距離は次のとおりです。

ボー レート - フィート
2400 – 400 ft.
4800 – 6,096.00 cm.
9600 – 3,048.00 cm.

ボー レート - フィート
19200 – 1,524.00 cm.
38400 – 762.00 cm.
57600 – 487.68 cm.
115200 – 243.84 cm.

ネットワーク速度の設定

KSX II におけるネットワーク速度の設定

ネットワーク スイッチにおけるポートの設定		自動	1000/全二重	100/全二重	100/半二重	10/全二重	10/半二重
	自動	使用可能な最高速度	1000/全二重	KSX II: 100/全二重 スイッチ: 100/半二重	100/半二重	KSX II: 10/全二重 スイッチ: 10/半二重	10/半二重
	1000/全二重	1000/全二重	1000/全二重	通信不可	通信不可	通信不可	通信不可
	100/全二重	KSX II: 100/半二重 スイッチ: 100/全二重	KSX II: 100/半二重 スイッチ: 100/全二重	100/全二重	KSX II: 100/半二重 スイッチ: 100/全二重	通信不可	通信不可
	100/半二重	100/半二重	100/半二重	KSX II: 100/全二重 スイッチ: 100/半二重	100/半二重	通信不可	通信不可
	10/全二重	KSX II: 10/半二重 スイッチ: 10/全二重	通信不可	通信不可	通信不可	10/全二重	KSX II: 10/半二重 スイッチ: 10/全二重
	10/半二重	10/半二重	通信不可	通信不可	通信不可	KSX II: 10/全二重 スイッチ: 10/半二重	10/半二重

凡例:

(白)	通信できません。
(緑)	サポート
(水色)	通信は行えますが、推奨できません。
(赤)	Ethernet 仕様でサポートされていません。通信は行えますが、衝突が発生します。
(太枠)	Ethernet 仕様では通信できないことになっています。KSX II は期待どおりに動作しません。

注:ネットワーク通信の信頼性を高めるため、KSX II とネットワーク スイッチの双方で、通信速度と通信方式を同じ設定にしてください。たとえば、KSX II とネットワーク スイッチで "自動検出" に設定するか (推奨)、または、双方の通信速度と通信方式を同じ設定にします (例: 100 Mbps/全二重)。

接続

KSX II を一般的なベンダ/モデルの組み合わせに接続するときに必要な KSX II ハードウェア (アダプタやケーブル) を次の表に示します。

ベンダ	デバイス	コンソール コネクタ	シリアル接続
チェックポイント	ファイアウォール	DB9M	ASCSDB9F アダプタと CAT 5 ケーブル
Cisco	PIX ファイアウォール	DB9M	ASCSDB9F アダプタと CAT 5 ケーブル
Cisco	Catalyst	RJ-45	CRLVR-15 ロールオーバー ケーブル、または CRLVR-1 アダプタ ケーブルと CAT5 ケーブル このコネクタを

ベンダ	デバイス	コンソール コネクタ	シリアル接続
			持つ KSX II-48 の各モデルのターミナル ポート (RJ-45 コネクタ タイプ) を別の KSX II に接続するための CRLVR-1 ケーブル。
Cisco	ルータ	DB25F	ASCSDB25M アダプタと CAT 5 ケーブル
Hewlett Packard®	UNIX® サーバ	DB9M	ASCSDB9F アダプタと CAT 5 ケーブル
Silicon Graphics	Origin		
Sun™	SPARCStation	DB25F	ASCSDB25M アダプタと CAT 5 ケーブル
Sun	Netra T1	RJ-45	CRLVR-15 ケーブル、または CRLVR-1 アダプタと CAT5 ケーブル
Sun	Cobalt	DB9M	ASCSDB9F アダプタと CAT 5 ケーブル
各種ベンダ	Windows NT®		

一般的に使用されるケーブルやアダプタの一覧については、Raritan の Web サイト (www.raritan.com) のサポート ページを参照してください。

KSX II のシリアル RJ-45 ピン配列

最大のポート密度を提供して簡単な UTP (カテゴリ 5) 配線にするため、KSX II では小型の RJ-45 ポートを介したシリアル接続ができます。ただし、RJ-45 を介したシリアル接続は、業界標準として広く採用されているわけではありません。

RJ-45 コネクタのピン配列を次の表に示します。

RJ-45 ピン	信号
1	RTS
2	DTR
3	TxD
4	GND
5	DCD
6	RxD
7	DSR
8	CTS

KSX II のシリアル ピン配列（RJ-45）についての最新情報は、Raritan Web サイト（www.raritan.com）のサポート ページを参照してください。

DB9F Null 化シリアルアダプタのピン配列

RJ-45 (メス)	DB9 (メス)
1	8
2	1, 6
3	2
4	SHELL
5	5
6	3
7	4
8	7

DB9M Null 化シリアルアダプタのピン配列

RJ-45 (メス)	DB9 (オス)
1	8
2	1, 6
3	2
4	SHELL

RJ-45 (メス)	DB9 (オス)
5	5
6	3
7	4
8	7

DB25F Null 化シリアルアダプタのピン配列

RJ-45 (メス)	DB25 (メス)
1	5
2	6, 8
3	3
4	1
5	7
6	2
7	20
8	4

DB25M Null 化シリアルアダプタのピン配列

RJ-45 (メス)	DB25 (オス)
1	5
2	6, 8
3	3
4	1
5	7
6	2
7	20
8	4

Ap B　LDAP/LDAPS スキーマの更新

重要:この章に記載されている手順は、経験豊富なユーザのみが行うようにしてください。

この章の内容

ユーザ グループ情報を返す 324
スキーマへの書き込み操作を許可するようにレジストリを設定する.. 325
新しい属性を作成する 326
属性をクラスに追加する 327
スキーマ キャッシュを更新する 328
ユーザ メンバの rciusergroup 属性を編集する 329

ユーザ グループ情報を返す

この章で説明する内容に従って、ユーザ認証の成功後にユーザ グループ情報を返すように設定してください。ユーザ グループ情報は、ユーザへの権限付与に役立ちます。

LDAP/LDAPS から返す場合

LDAP/LDAPS 認証に成功すると、KSX II では、そのユーザの所属グループに付与されている権限に基づいて、そのユーザに付与する権限が決まります。リモート LDAP サーバから次のような属性が返されるので、ユーザ グループ名がわかります。

rciusergroup　　attribute type: string

このように属性を返すには、LDAP/LDAPS サーバ上でスキーマを拡張しなければならないことがあります。認証サーバ管理者に連絡し、この属性を有効にしてください。

また、Microsoft® Active Directory® の場合、標準 LDAP memberOf が使用されます。

Microsoft Active Directory から返す場合

注:この手順は、経験豊富な Active Directory® 管理者だけが行ってください。

Windows 2000® オペレーティング システム サーバ 上の Microsoft® Active Directory からユーザ グループ情報を返すには、LDAP/LDAPS スキーマを更新する必要があります。詳細については、Microsoft 発行のドキュメントを参照してください。

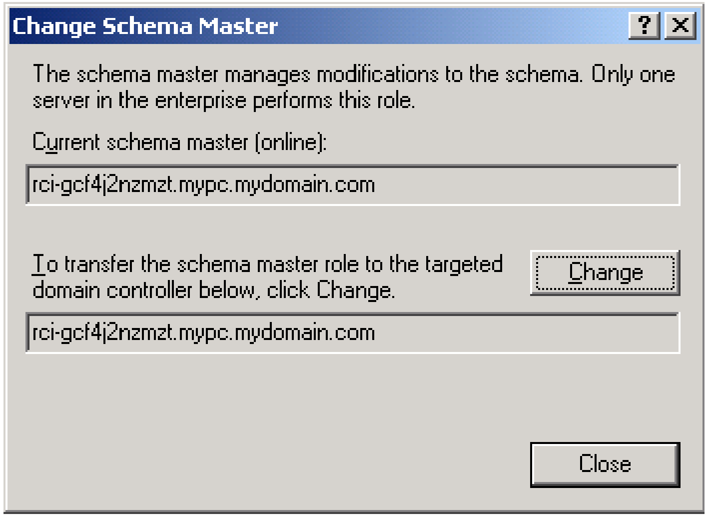
1. Active Directory 用のスキーマ プラグインをインストールします。インストール手順については、Active Directory のドキュメントを参照してください。
2. Active Directory コンソールを起動し、[Active Directory Schema] (Active Directory スキーマ) を選択します。

スキーマへの書き込み操作を許可するようにレジストリを設定する

ドメイン コントローラによるスキーマへの書き込みを許可するため、スキーマの更新を許可するレジストリ エントリを設定する必要があります。

▶ スキーマへの書き込みを許可するには

1. ウィンドウの左ペインで [Active Directory Schema] (Active Directory® スキーマ) ルート ノードを右クリックし、コンテキスト メニューの [Operations Master] (操作マスタ) をクリックします。[Change Schema Master] (スキーマ マスタの変更) ダイアログ ボックスが開きます。



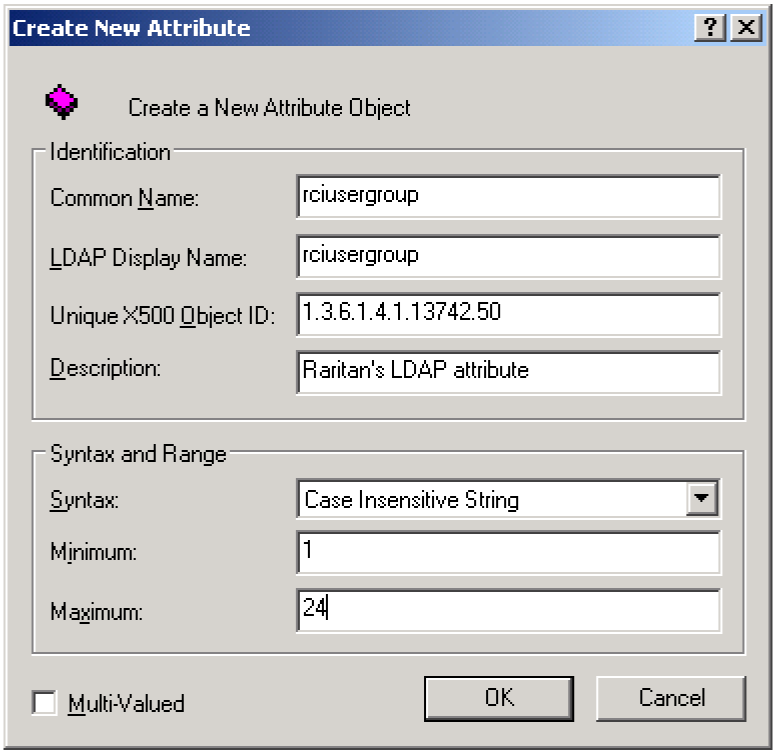
2. [Schema can be modified on this Domain Controller] (このドメイン コントローラでスキーマを修正できるようにする) チェック ボックスをオンにします。**(オプション)**

3. [OK] をクリックします。

新しい属性を作成する

▶ rciusergroup クラスに対する新しい属性を作成するには

1. ウィンドウの左ペインで、[Active Directory Schema] (Active Directory® スキーマ) の前に表示されている [+] (+) 記号をクリックします。
2. 左ペインで [Attributes] (属性) を右クリックします。
3. コンテキスト メニューの [New] (新規) をクリックし、続いて [Attribute] (属性) をクリックします。警告メッセージが表示されたら、[Continue] (続行) をクリックします。[Create New Attribute] (属性の新規作成) ダイアログ ボックスが開きます。



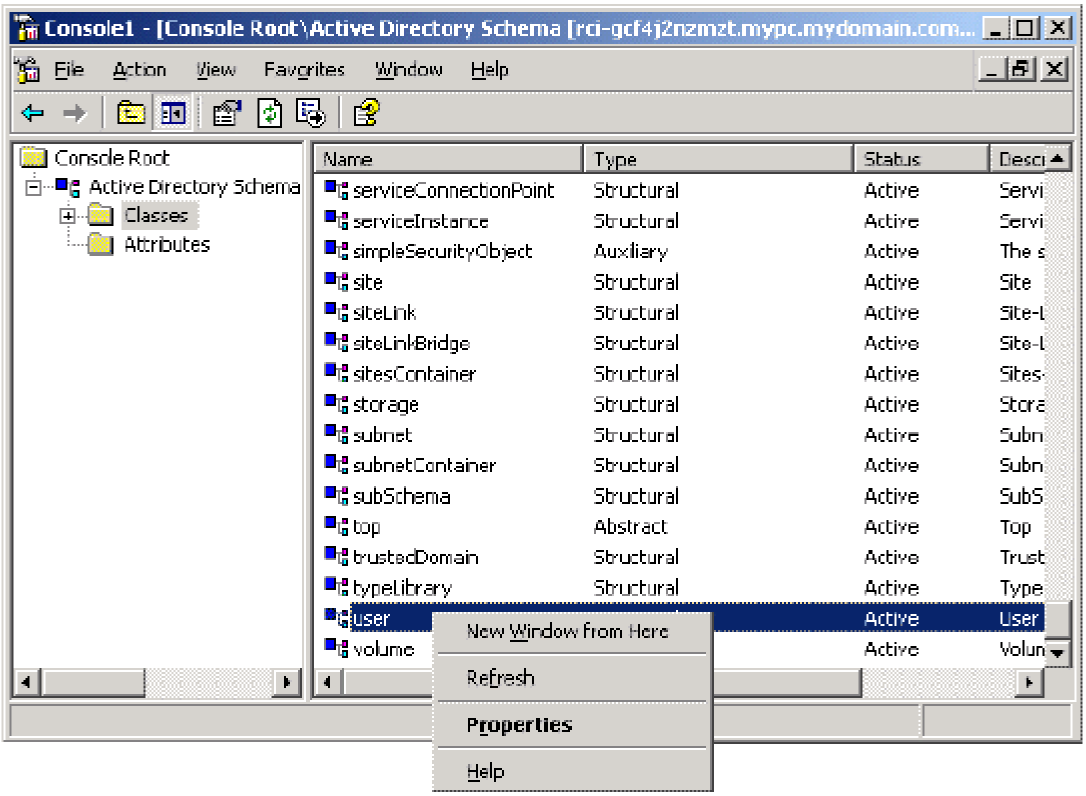
4. [Common Name] (共通名) ボックスに「rciusergroup」と入力します。
5. [LDAP Display Name] (LDAP 表示名) ボックスに「rciusergroup」と入力します。
6. [Unique X500 Object ID] (一意の X.500 オブジェクト ID) フィールドに「1.3.6.1.4.1.13742.50」と入力します。
7. [Description] (説明) ボックスにわかりやすい説明を入力します。
8. [Syntax] (構文) ボックスの一覧で [Case Insensitive String] (大文字/小文字の区別がない文字列) を選択します。

9. [Minimum] (最小) ボックスに「1」と入力します。
10. [Maximum] (最大) ボックスに「24」と入力します。
11. [OK] をクリックし、新しい属性を作成します。

属性をクラスに追加する

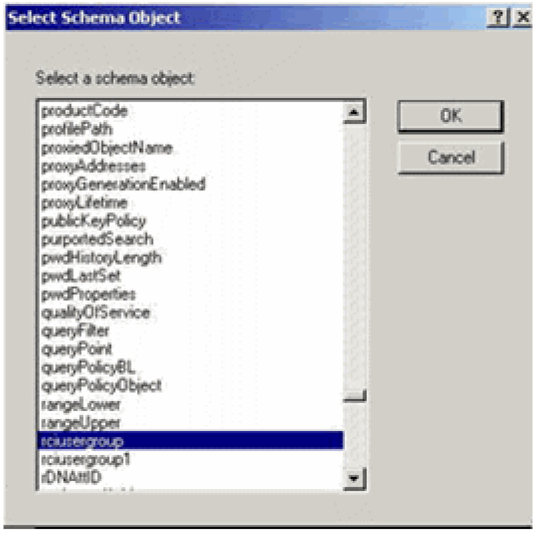
▶ 属性をクラスに追加するには

1. ウィンドウの左ペインで [Classes] (クラス) をクリックします。
2. 右ペインをスクロールして [user] (user) を表示し、右クリックします。



3. コンテキスト メニューの [Properties] (プロパティ) をクリックします。[user Properties] (user のプロパティ) ダイアログ ボックスが開きます。
4. [Attributes] (属性) タブをクリックしてそのプロパティ ページを開きます。
5. [Add] (追加) をクリックします。

6. [Select a schema object] (スキーマ オブジェクトを選択) ボックスの一覧で [rciusergroup] (rciusergroup) を選択します。



7. [Select Schema Object] (スキーマ オブジェクトを選択) ダイアログ ボックスで [OK] をクリックします。
8. [user Properties] (user のプロパティ) ダイアログ ボックスで [OK] をクリックします。

スキーマ キャッシュを更新する

▶ スキーマ キャッシュを更新するには

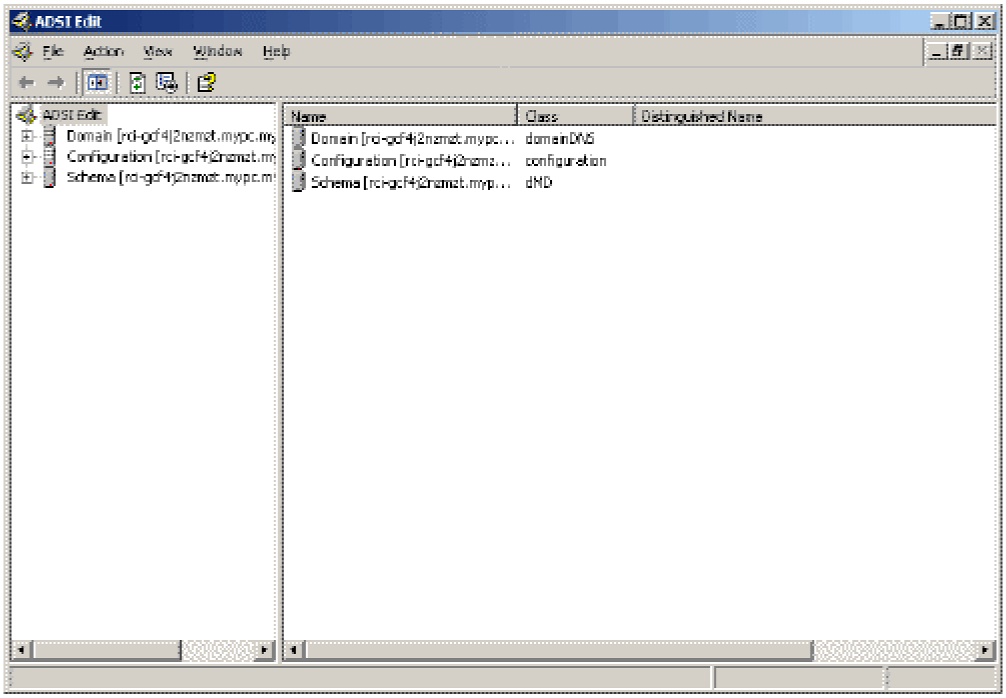
1. ウィンドウの左ペインで [Active Directory Schema] (Active Directory® スキーマ) を右クリックし、コンテキスト メニューの [Reload the Schema] (スキーマを再ロード) を選択します。
2. Active Directory スキーマ MMC コンソール (Microsoft® Management Console) を最小化します。

ユーザ メンバの rciusergroup 属性を編集する

Windows Server 2003® 上で Active Directory® スクリプトを実行するには、Microsoft® から提供されるスクリプトを使用します（Windows Server 2003 のインストール用 CD-ROM に収録されています）。これらのスクリプトは、Microsoft® Windows 2003 のインストール時にシステムにロードされます。Active Directory Service Interface (ADSI) は、Active Directory の下位レベルのエディタとして動作します。これにより、オブジェクトの追加、削除、移動などの一般的な管理作業を、ディレクトリ サービスを使用して行うことができます。

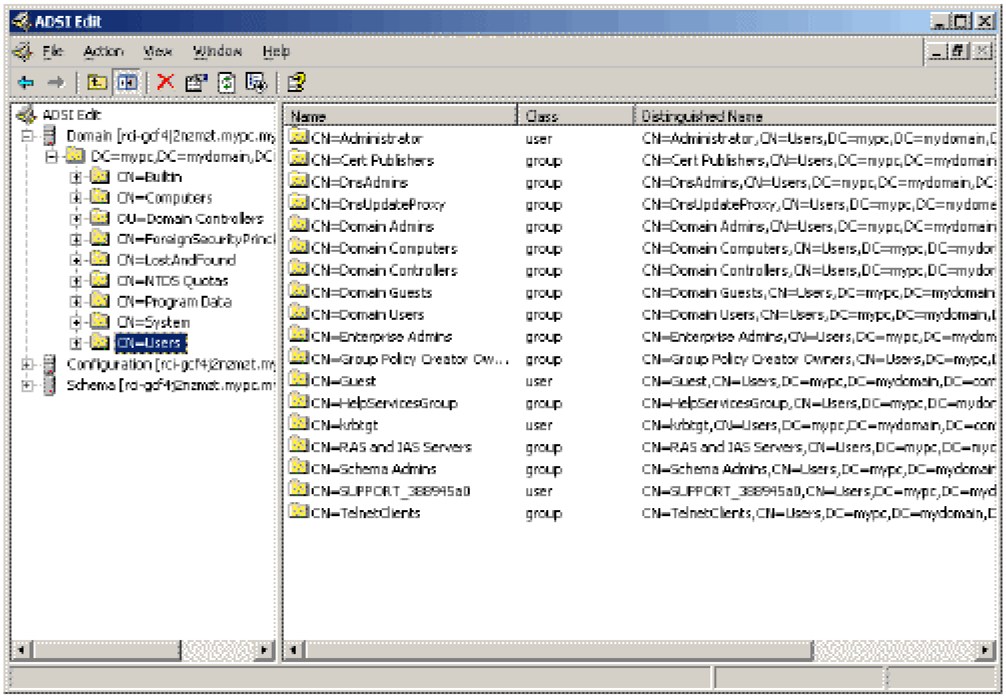
▶ rciusergroup グループ内の個別のユーザ属性を編集するには、以下の手順に従います。

1. Windows Server 2003 のインストール用 CD-ROM を挿入し、エクスプローラで Support フォルダの下の Tools フォルダを開きます。
2. SUPTOOLS.MSI をダブルクリックし、サポート ツールをインストールします。
3. サポート ツールがインストールされたフォルダを開きます。adsiedit.msc を実行します。[ADSI Edit] (ADSI 編集) ウィンドウが開きます。



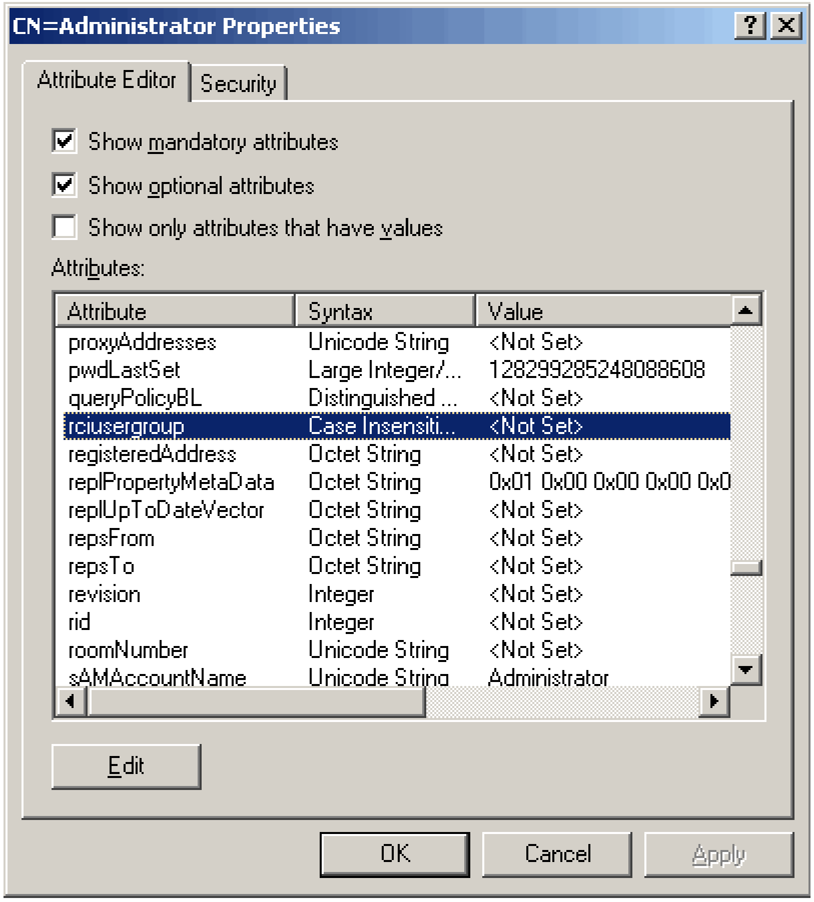
4. [Domain] (ドメイン) を開きます。

5. ウィンドウの左ペインで CN=Users フォルダを選択します。



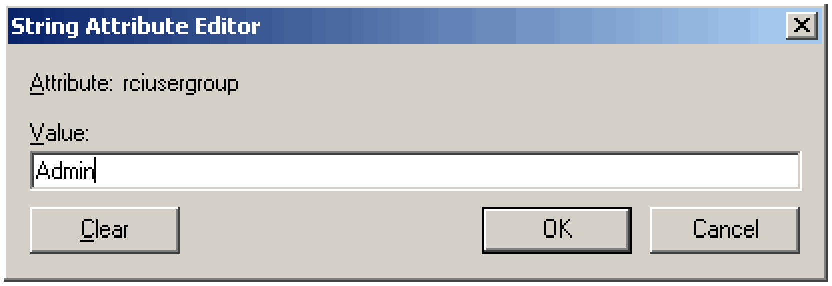
6. 右ペインで、プロパティ値を編集したいユーザ名を探します。ユーザ名を右クリックし、コンテキスト メニューの [Properties] (プロパティ) をクリックします。

7. [Attribute Editor] (属性エディタ) タブをクリックします。[Attributes] (属性) ボックスの一覧で [rciusergroup] (rciusergroup) を選択します。



8. [Edit] (編集) をクリックします。[String Attribute Editor] (文字列属性エディタ) ダイアログ ボックスが開きます。

9. [Value] (値) ボックスに、KSX II で作成したユーザ グループを入力します。[OK] をクリックします。



Ap C　留意事項

この章の内容

概要 332
Java 332
オペレーティング システムの IPv6 のサポートに関する留意事項 335
キーボード 336
Dell 筐体を接続する場合のケーブル長と画面解像度 339
ブラウザに関する留意事項 340
USB ポートおよびプロファイルに関する留意事項 341
SUSE と VESA のビデオ モード 343
CIM に関する留意事項 344
仮想メディアに関する留意事項 344
CC-SG に関する留意事項 345

概要

この章では、KSX II の使用に関する重要事項について説明します。今後更新される情報については、弊社 Web サイトで提供されます。更新情報を表示するには、KSX II リモート コンソールの [Help] (ヘルプ) リンクをクリックしてください。

注:このセクションの一部のトピックでは、記載されている情報がさまざまなデバイスに影響を与えるため、他の複数の Raritan デバイスにも言及しています。

Java

AES (256 ビット) を使用する際の前提条件と Java のサポート対象構成

アプリケーション	前提条件	サポート
スタンドアロン MPC	Java Cryptography Extension® (JCE®) 無制限強度の管轄ポリシー ファイルをインストールする必要があります。+	はい
スタンドアロン RSC	Java Cryptography Extension (JCE)	はい

<table>
<tr><th>アプリケーション</th><th>前提条件</th><th>サポート</th></tr>
<tr><td></td><td>無制限強度の管轄ポリシー ファイルをインストールする必要があります。+</td><td></td></tr>
<tr><td>MPC アプレット</td><td>Java Cryptography Extension (JCE) 無制限強度の管轄ポリシー ファイルをインストールする必要があります。+</td><td><table>
<tr><th>ブラウザ</th><th>サポート</th></tr>
<tr><td>Firefox® 2.0.0.7</td><td>はい</td></tr>
<tr><td>Firefox 3.0.x</td><td>はい</td></tr>
<tr><td>Internet Explorer® 6*</td><td>いいえ</td></tr>
<tr><td>Internet Explorer 7</td><td>はい</td></tr>
<tr><td>Internet Explorer 8</td><td>はい</td></tr>
</table></td></tr>
<tr><td>HTML アクセス クライアント</td><td>Java Cryptography Extension (JCE) 無制限強度の管轄ポリシー ファイルをインストールする必要があります。+</td><td><table>
<tr><th>ブラウザ</th><th>サポート</th></tr>
<tr><td>Firefox 2.0.0.7</td><td>はい</td></tr>
<tr><td>Firefox 3.0.x</td><td>はい</td></tr>
<tr><td>Internet Explorer 6 *</td><td>いいえ</td></tr>
<tr><td>Internet Explorer 7</td><td>はい</td></tr>
<tr><td>Internet Explorer 8</td><td>はい</td></tr>
</table></td></tr>
</table>

+ 各種 JRE™ の管轄ファイルは、Java™ Sun™ サイトの [その他のダウンロード] で入手できます。

JRE	リンク
JRE1.6	http://java.sun.com/javase/downloads/index.jsp

* IE6 は AES 128 をサポートしていません。

Java Runtime Environment (JRE)

重要: Java のキャッシュ機能を無効にし、Java™ キャッシュをクリアすることを推奨します。詳細については、Java のマニュアルを参照してく

ださい。

KSX II リモート コンソールおよび Multi-Platform Client (MPC) を実行するには、JRE™ が必要です。Java Runtime Environment™ (JRE) version 1.6.x 以降がサポートされています。KSX II リモート コンソールでは、Java のバージョンが検査されます。バージョンが不適切であるかまたは古い場合、互換性のあるバージョンをダウンロードするよう指示されます。

注: 多言語対応のキーボードを KSX II リモート コンソール (Virtual KVM Client (VKC)) で使用できるようにするには、多言語バージョンの JRE をインストールする必要があります。

オペレーティング システムの **IPv6** のサポートに関する留意事項

Java

Java™ 1.7 では、次のオペレーティング システム (OS) に対して IPv6 がサポートされています。

- Solaris™ 10 (以降)
- Linux® カーネル 2.1.2 (以降)/RedHat 6.1 (以降)
- Solaris 10 (以降)
- Windows XP® SP1、Windows 2003®、Windows Vista®、および Windows 7

Java では、次の IPv6 構成は*サポートされていません*。

- Microsoft® Windows® 上の J2SE では、IPv6 はサポートされていません。

Linux

- IPv6 を使用する場合、Linux カーネル 2.4.0 以降を使用することを推奨します。
- IPv6 対応のカーネルをインストールするか、または、IPv6 関連オプションを有効にしてカーネルを再ビルドする必要があります。
- IPv6 を使用する場合、Linux 用のネットワーク ユーティリティをいくつかインストールする必要があります。詳細については、http://www.bieringer.de/linux/IPv6/IPv6-HOWTO/IPv6-HOWTO.html を参照してください。

Windows

- Windows XP ユーザや Windows 2003 ユーザは、Microsoft の IPv6 対応サービス パックをインストールし、IPv6 を有効にする必要があります。
- Windows XP に IPv6 を搭載した AKC の場合は、ファイアウォールの例外リストに実行可能ファイル kxgui.exe を追加します。クライアントのログ ファイルを表示し、ファイル kxgui.exe の場所の完全パスを確認します。

Samba

- Samba を使用する場合、IPv6 と仮想メディアを併用することはできません。

キーボード

アメリカ英語以外のキーボード

フランス語キーボード

キャレット記号 (Linux® クライアントのみ)

Linux® クライアントとフランス語キーボードを併用する場合、 では Alt Gr + 9 というキー組み合わせがキャレット記号 (^) として処理されません。

▶ キャレット記号を入力するには

フランス語キーボードの ^ キー (P キーの右にある) を押し、すぐに Space キーを押します。

次のコマンドを実行するマクロを作成する方法もあります。

1. 右 Alt キーを押す。
2. 9 キーを押す。
3. 9 キーを離す。
4. 右 Alt キーを離す。

注:これらの手順は、母音の上に付ける曲折アクセントには当てはまりません。フランス語キーボードで ^ キーと他の文字を組み合わせて使用した場合、曲折アクセントになります。

アクセント記号 (Windows XP® クライアントのみ)

Windows XP® クライアントでフランス語キーボードを使用する場合、 で Alt Gr + 7 というキー組み合わせを使用すると、アクセント記号付き文字が 2 つ表示されます。

注:この現象は、Linux® クライアントでは発生しません。

数字キーパッド

でフランス語キーボードを使用する場合、数字キーパッドにある記号は次のとおりに表示されます。

数字キーパッド上の記号キー	表示
/	;
.	;

ティルデ記号

でフランス語キーボードを使用する場合、Alt Gr + 2 というキー組み合わせがティルデ記号（˜）として処理されません。

▶ ティルデ記号を入力するには

次のコマンドを実行するマクロを作成します。

- 右 Alt キーを押す。
- 2 キーを押す。
- 2 キーを離す。
- 右 Alt キーを離す。

キーボード言語の設定 (Fedora クライアント)

Linux® 版の JRE™ には、[System Preferences] (システム基本設定) で設定した外国語キーボードに対して正しいキー イベントが生成されない、という問題があります。したがって、次の表に示す方法を使用して外国語キーボードを設定することを推奨します。

言語	設定方法
アメリカ英語/国際	デフォルト設定
イギリス英語	[System Settings] (システム設定) (Control Center)
フランス語	Keyboard Indicator
ドイツ語	Keyboard Indicator
ハンガリー語	[System Settings] (システム設定) (Control Center)
スペイン語	[System Settings] (システム設定) (Control Center)
ドイツ語（スイス）	[System Settings] (システム設定) (Control Center)
ノルウェー語	Keyboard Indicator
スウェーデン語	Keyboard Indicator
デンマーク語	Keyboard Indicator
日本語	[System Settings] (システム設定) (Control Center)
韓国語	[System Settings] (システム設定) (Control

言語	設定方法
アメリカ英語/国際	デフォルト設定
	Center)
スロベニア語	[System Settings] (システム設定) (Control Center)
イタリア語	[System Settings] (システム設定) (Control Center)
ポルトガル語	[System Settings] (システム設定) (Control Center)

注: デスクトップ環境として Gnome を使用している Linux システムでは、Keyboard Indicator を使用してください。

Linux クライアントでハンガリー語キーボードを使用している場合、ダブル アキュート付き U およびダブル アキュート付き O は、JRE 1.6 でのみ入力できます。

Fedora® クライアントでは、キーボード言語を設定する方法がいくつかあります。VKC および MPC でキーを正しく対応付けるには、次に示す方法を使用します。

▶ [System Settings] (システム設定) を使用してキーボード言語を設定するには

1. ツールバーで [System] (システム) > [Preferences] (基本設定) > [Keyboard] (キーボード) を選択します。
2. [Layouts] (レイアウト) タブをクリックします。
3. 言語を追加または選択します。
4. [Close] (閉じる) をクリックします。

▶ Keyboard Indicator を使用してキーボード言語を設定するには

1. タスク バーを右クリックし、[Add to Panel] (パネルに追加) をクリックします。
2. [Add to Panel] (パネルに追加) ダイアログ ボックスで、Keyboard Indicator を右クリックし、メニューの [Open Keyboard Preferences] (キーボード基本設定) をクリックします。
3. [Keyboard Preferences] (キーボード基本設定) ダイアログ ボックスで、[Layouts] (レイアウト) タブをクリックします。
4. 必要に応じて言語を追加または削除します。

組み合わせと JRE

Java Runtime Environment™ (JRE™) の制限により、Fedora®、Linux®、および Solaris™ クライアントは、英語 (イギリス) および英語 (インターナショナル) キーボードの Alt Gr から無効な応答を受け取ります。Fedora、Linux、または Solaris で Java™ 1.5 を使用している場合、Alt Gr キーを押しながら他のキーを押したときに生成されるイベントが、受け付けられません。Java 1.6 ではこの点が改善されているように見えますが、keyPressed イベントおよび keyReleased イベントでは、Alt Gr キーが "不明なキー コード" として扱われます。

また、Alt Gr キーを押しながら別のキーを押した場合 (たとえばイギリス英語キーボードでは、Alt Gr キーを押しながら 4 キーを押すと、ユーロ記号が入力されます)、keyTyped イベントが生成され、続いて keyReleased イベントが生成されます。keyPressed イベントは生成されません。Java 1.6 ではこの点を改善するため、keyPressed イベントも生成されるようになりました。

Macintosh キーボード

クライアントとして Macintosh® を使用している場合、Macintosh キーボードの次のキーは、JRE™ によって取り込まれません。

- F9
- F10
- F11
- F14
- F15
- Volume Up
- Volume Down
- Mute
- Eject

つまり、Macintosh クライアントのキーボードでこれらのキーが押されても、VKC および MPC では処理できません。

Dell 筐体を接続する場合のケーブル長と画面解像度

KSX II に Dell® 製ブレード筐体を接続する場合、画質を維持するために次のケーブル長と画面解像度を使用することを推奨します。

画面解像度	ケーブル長
1024x768@60Hz	15.24 m (50 フィート)
1280x1024@60Hz	15.24 m (50 フィート)
1600x1200、60Hz	9.14 m (30 フィート)

ブラウザに関する留意事項

Fedora Core のフォーカスに関する問題を解決する

MPC を使用しているときに、LX、KX II、または KSX II デバイスにログインできなくなったり、Windows® や SUSE を実行している KVM ターゲット サーバにアクセスできなくなったりすることがあります。また、Ctrl + Alt + M キーを押してもキーボード ショートカット メニューが表示されないことがあります。このような問題が発生するのは、Fedora® Core 6 と Firefox® 1.5 または 2.0 を組み合わせて使用している場合です。

Raritan でテストした結果、libXp をインストールすれば Fedora Core 6 のウィンドウ フォーカスに関する問題を解決できることがわかりました。Raritan がテストで使用したのは libXp-1.0.0.8.i386.rpm です。この libXp をインストールした結果、ウィンドウ フォーカスとポップアップ メニューに関する問題がすべて解決しました。

注: libXp は、SeaMonkey (旧称: Mozilla®) ブラウザで Java™ プラグインを使用する場合にも必要となります。

マウス ポインタの同期 (Fedora)

Fedora® 7 を実行しているターゲット サーバにデュアル マウス モードで接続しているときに、ターゲット サーバとローカルのマウス ポインタが同期しなくなった場合、マウス モードをインテリジェント モードに、またはインテリジェント モードから標準モードに変更すると同期が回復することがあります。

シングル マウス モードを使用すると、制御しやすくなります。

▶ マウス ポインタを再度同期させるには、以下の手順に従います。

- Virtual KVM Client (VKC) の [Synchronize Mouse] (マウスを同期) オプションを使用します。

Fedora サーバへの VKC および MPC のスマート カード接続

MPC または VKC でスマート カードを使用して Fedora® サーバに接続する場合は、pcsc-lite ライブラリを 1.4.102-3 以降にアップグレードします。

注: この機能は、KSX II 2.3.0 (以降) および KX II 2.1.10 (以降) で提供されます。

Fedora 使用時の Firefox のフリーズに関する問題の解決

Fedora® サーバを使用している場合に Firefox® にアクセスすると、Firefox を開くときに Firefox がフリーズすることがあります。

この問題を解決するには、libnpjp2.so という Java™ プラグインをサーバにインストールします。

USB ポートおよびプロファイルに関する留意事項

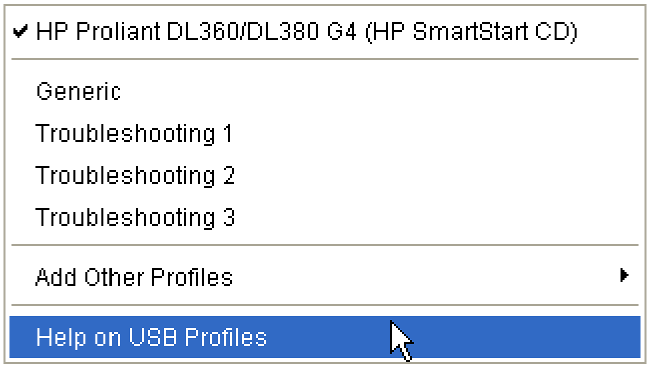
VM-CIM および DL360 の USB ポート

HP® DL360 サーバの背面と前面には、USB ポートがそれぞれ 1 つあります。DL360 では、両方の USB ポートを同時に使用することはできません。つまり、DL360 サーバに対してデュアル VM-CIM を使用することはできません。

ただし、代替策として、DL360 サーバの背面の USB ポートに USB2 ハブを接続し、そのハブにデュアル VM-CIM を接続することはできます。

USB プロファイルの選択に関するヘルプ

Virtual KVM Client (VKC) で KVM ターゲット サーバに接続しているとき、[USB Profile] (USB プロファイル) メニューの [Help on USB Profiles] (USB プロファイルに関するヘルプ) をクリックすると、USB プロファイルに関する情報が表示されます。



USB プロファイルに関するヘルプは、[USB Profile Help] (USB プロファイルに関するヘルプ) ウィンドウに表示されます。個々の USB プロファイルの詳細については、「*選択可能な USB プロファイル* 『*116*p. の"*使用できる USB プロファイル*"参照 』」を参照してください。

サーバで使用されている多様な OS および BIOS に対応する USB プロファイルが、標準で用意されています。このため、リモート USB デバイスとターゲット サーバを最適な方法で対応付けることができます。

"Generic" プロファイルは、一般に使用されているほとんどのターゲット サーバ構成のニーズに対応しています。

その他のプロファイルは、一般的に展開される他のサーバ設定 (例: Linux® や Mac OS X®) の特定のニーズを満たすように提供されています。

さらに、ターゲット サーバが BIOS レベルで動作しているときなどに仮想メディア機能の互換性を高めるための、さまざまなプロファイルが用意されています (プロファイルの名前がプラットフォーム名と BIOS のリビジョンで構成されている)。

[Add Other Profiles] (他のプロファイルを追加) をクリックすると、システムで使用可能なその他のプロファイルが一覧表示されます。この一覧で設定したプロファイルは、[USB Profile] (USB プロファイル) メニューに追加されます。この一覧には、トラブルシューティング用プロファイルのセットがあります。これらのプロファイルは、構成における制限事項を明確化するのに役立ちます。

[USB Profile] (USB プロファイル) メニューの項目を変更するには、KSX II ローカル コンソールまたは KSX II リモート コンソールの [Device Settings] (デバイス設定) メニューの [Port Configuration] (ポート設定) ページを使用します。

Raritan から提供されている標準の USB プロファイルがどれもターゲット サーバの要件を満たさない場合、Raritan のテクニカル サポート部門がお客様と協力し、そのターゲット サーバに対する解決策を探ることができます。次の手順を実行することを推奨します。

1. Raritan の Web サイト (www.raritan.com) の [Firmware Upgrade] (ファームウェアのアップグレード) ページで最新のリリース ノートを調べ、ご使用のターゲット サーバ構成に合った解決策が提供されているかどうかを確認します。
2. 提供されていない場合は、Raritan のテクニカル サポート部門に問い合わせます。その際、次の情報を準備してください。
    a. ターゲット サーバに関する情報 (製造元、モデル、BIOS、およびバージョン)。
    b. 用途 (例: イメージをリダイレクトし、サーバの OS を CD-ROM から再ロードする)。

スマート カード リーダー使用時の USB プロファイルの変更

ターゲット サーバの USB プロファイルの変更が必要になる場合があります。たとえば、接続速度が [High Speed USB] (高速 USB) のときにターゲットに問題が発生する場合、接続速度を [Use Full Speed for Virtual Media CIM] (仮想メディア CIM でフル スピードを使用) に変更する必要があります。

プロファイルを変更すると、「新しいハードウェアが検出されました」というメッセージが表示されることがあります。この場合は、管理者権限でターゲットにログインして USB ドライバを再インストールする必要があります。この現象は、ターゲットで USB デバイスの新しい設定が検出される最初の数回だけ発生する可能性があります。その後はターゲットによって正しいドライバが選択されます。

SUSE と VESA のビデオ モード

SUSE の X.org 設定ツールである SaX2 を実行すると、X.org 設定ファイル内の Monitor セクションの Modeline エントリにビデオ モードが書き込まれます。これらのビデオ モードは、VESA モニタを選択している場合であっても、VESA のビデオ モード タイミングと正確に対応していません。一方 KSX II では、正確に同期させるため、VESA のビデオ モード タイミングが使用されています。このビデオ モード タイミングの不一致により、黒の境界線が表示される、画面の一部が表示されない、ノイズが発生する、などの問題が発生することがあります。

▶ SUSE のビデオ表示を設定するには

1. 生成された設定ファイル /etc/X11/xorg.conf 内に Monitor セクションがあり、その中に UseModes というオプションがあります。たとえば、
   UseModes "Modes[0]" と書き込まれています。
2. この行の先頭に # を付加してコメント行にするか、または、この行全体を削除します。
3. X サーバを再起動します。

これにより、X サーバの内部ビデオ モード タイミングが使用されるようになるので、VESA のビデオ モード タイミングと正確に対応します。この結果、KSX II 経由で画面が正しく表示されます。

CIM に関する留意事項

Linux ターゲット サーバに対して Windows の 3 ボタン マウスを使用する場合

Linux® ターゲット サーバに接続している Windows® クライアントで 3 ボタン マウスを使用する場合、左マウス ボタンがその 3 ボタン マウスの中央ボタンに対応付けられることがあります。

仮想メディアに関する留意事項

Dell OptiPlex および Dimension コンピュータ

Dell OptiPlex™ および Dimension コンピュータの中には、リダイレクトされたドライブ/ISO イメージからターゲット サーバを起動したり、[Port] (ポート) ページから [Use Full Speed for Virtual Media CIM] (仮想メディア CIM でフル スピードを使用) オプションを有効にしない限り) 仮想メディア セッションがアクティブな場合にターゲット サーバの BIOS にアクセスできなくなるものがあります。

注: Raritan は ISO9660 形式を標準でサポートしています。ただし、その他の CD-ROM 拡張でも動作します。

Windows 2000 の仮想メディアへのアクセス

D2CIM-VUSB を使用して Windows 2000® サーバ上の仮想メディアに仮想メディア ローカル ドライブにアクセスすることはできません。

ファイル追加後に仮想メディアが最新の情報に更新されない

仮想メディア ドライブがマウントされた後、そのドライブにファイルを追加した場合、ターゲット サーバ側でそのファイルがすぐに表示されないことがあります。表示するには、仮想メディア接続をいったん解除し、再確立します。

仮想メディア機能利用時におけるターゲット サーバの BIOS の起動時間

ターゲット サーバにおいてメディアが仮想マウントされている場合、そのターゲット サーバの BIOS の起動に要する時間が長くなることがあります。

▶ 起動に要する時間を短縮するには

1. VKC を終了し、仮想メディア ドライブを完全に解放します。
2. ターゲット サーバを再起動します。

高速の仮想メディア接続を使用した場合の仮想メディアの接続エラー

[High Speed USB] (高速 USB) 接続でターゲットに問題が発生する場合、またはターゲットで接続やケーブルの追加に起因する信号劣化により USB プロトコル エラーが発生する場合は、[Use Full Speed for Virtual Media CIM] (仮想メディア CIM でフル スピードを使用) の選択が必要になることがあります。(たとえば、ドングルを介したブレード サーバへの接続)。

CC-SG に関する留意事項

VKC のバージョンが CC-SG プロキシ モードで認識されない

Virtual KVM Client (VKC) を CommandCenter Secure Gateway (CC-SG) からプロキシ モードで起動した場合、VKC のバージョンは認識されません。

[About Raritan Virtual KVM Client] (VKC のバージョン情報) ダイアログ ボックスで、バージョンが "Version Unknown" (不明なバージョン) と表示されます。

シングル マウス モード: CC-SG の管理下にあるターゲットに接続する場合

Firefox® と DCIM-PS2 または DCIM-USBG2 を使用して、CC-SG の管理下にある KSX II ターゲットに接続しているとき、Virtual KVM Client (VKC) でシングル マウス モードに切り替えると、VKC ウィンドウからフォーカスが外れ、マウスが応答しなくなります。

この場合、マウスの左ボタンをクリックするかまたは Alt キーを押しながら Tab キーを押し、フォーカスを VKC ウィンドウに戻します。

デバイスのポート間の移動

同じ Raritan デバイスのポート間で移動し、1 分以内に管理作業を再開した場合、CC-SG によってエラー メッセージが表示されることがあります。

管理作業を再開すると、最新の情報に更新されます。

Ap D　FAQ

この章の内容

全般的な質問 347
シリアル アクセス 349
ユニバーサル仮想メディア 355
USB プロファイル 356
IPv6 ネットワーキング 358
リモート アクセス 360
Ethernet と IP ネットワーキング 362
サーバ 366
ブレード サーバ 366
インストール 369
ローカル ポート 371
電源制御 373
拡張性 374
セキュリティ 375
スマート カード認証と CAC 認証 377
管理機能 378
その他 379

全般的な質問

KSX II とは何ですか。

KSX II は第 2 世代のデジタル KVM (キーボード/ビデオ/マウス) スイッチです。IT 管理者は BIOS レベルの機能を使用して、ネットワーク上の 8、16、32、または 64* 台のサーバにアクセスし、制御できます。KSX II ではハードウェアと OS が完全に独立しているため、サーバがダウンしているときでも、ユーザはトラブルシューティングや再設定を行えます。

KSX II をラックに収容した場合、従来型のアナログ KVM スイッチと同等の機能性と利便性が維持されるだけでなく、省スペース効果とコスト節約効果が生まれます。また、KSX II には業界最高のパフォーマンスを誇る KVM-over-IP 技術が組み込まれているため、複数の管理者がネットワーク上のワークステーションでサーバの画面を表示することができます。

KSX II ではハードウェアと OS が完全に独立しているため、サーバがダウンしているときでも、ユーザはトラブルシューティングや再設定を行えます。

KSX II とリモート制御ソフトウェアの違いは何ですか。

KSX II をリモートで使用する場合、一見すると、画面がリモート制御ソフトウェア (例: pcAnywhere™、Windows Terminal Services/Remote Desktop®、VNC) に似ているように感じることがあります。しかし、KSX II はソフトウェアではなくハードウェア製品なので、これらのソフトウェアよりもはるかに高い機能を備えています。次に例を示します。

- OS やハードウェアに依存しない: KSX II を使用して、Windows®、Linux®、Solaris™ などを実行している Intel®、Sun™、PowerPC など、一般的なさまざまなオペレーティング システムを実行しているサーバを管理できます。
- ターゲット サーバの稼動状態に依存せず、エージェントも不要: KSX II を使用する際、ターゲット サーバ上でオペレーティング システムを起動しておく必要がありません。ターゲット サーバに特別なソフトウェアをインストールする必要もありません。
- アウトオブバンド: ターゲット サーバ上のネットワーク接続が使用不能になっている場合でも、KSX II から管理できます。
- BIOS レベルのアクセス: ターゲット サーバが起動中にハングした場合、ターゲット サーバをセーフ モードで起動する必要がある場合、または、システム BIOS のパラメータ値を修正する必要がある場合でも、KSX II は問題なく動作するので、これらの設定を行うことができます。
- 独立した OS とハードウェア – KSX II を使用して、Windows、Linux、Solaris などを実行している Intel、Sun、PowerPC など、一般的なさまざまなオペレーティング システムを実行しているサーバを管理できます。

KSX I にない、KSX II の特徴は何ですか。

KSX II には、仮想メディア、デュアル ギガビット Ethernet、次世代ローカル ポート、シリアル ポートの拡張サポートなどの優れた機能が多数追加されています。

Dominion KSX I から KSX II に移行するにはどうすればよいですか。

一般に、お客様には既存のスイッチを長期間お使いいただけます。データ センタを拡張する場合、お客様は新しい KSX II モデルを購入して使用することが考えられます。Raritan の集中管理ユニットである CommandCenter Secure Gateway および Multi-Platform Client (MPC) は、KSX I スイッチおよび KSX II スイッチを継続してサポートしています。

KSX II スイッチでサポートされているのはどの CIM ですか。

「*サポートされているオペレーティング システムおよび CIM (KVM ターゲット サーバ)* 『*299*p. 』」を参照してください。

KSX II はラックに収容できますか。

はい。KSX II には、19 インチ ラック マウント ブラケットが標準で同梱されています。また、逆向きに収容して、サーバ ポートがある面を前にすることもできます。

KSX II の寸法はどのくらいですか。

KSX II の高さはわずか 1U であり、標準の 19 インチ ラックに収容できます。奥行きはわずか 29 cm です。

シリアル アクセス

Dominion KSX II でネットワーク アドレスを設定し、IP を正常に Ping できますが、Web ブラウザを使ってアクセスしようとすると、「Page cannot be found or server error, contact System Administrator. (ページが見つからないか、サーバ エラーが発生しました。システム管理者に連絡してください。)」というメッセージが表示されます。

Web ブラウザの設定を確認し、プロキシ サーバが使用されていることを確認してください。その場合、[Bypass local addresses or configure KSX IP in the exception list] (ローカル アドレスをバイパスするか、例外リスト内の KSX IP を設定する) のチェックボックスをクリックします。次に、Web ブラウザが 128 ビットの暗号強度を備えているか確認してください。この情報を確認するには、[Help] (ヘルプ) メニューから、[About] (製品情報) をクリックします。

Raritan Console (KSX II 上) の [Emulator] (エミュレータ) メニューで、[Send Break] (ブレークの送信) オプションを選択しても、Sun™ サーバにブレークが送信されません。何が問題で、どうすればその問題を見つけることができますか。

SUN のマシンがブレーク信号に応答しない場合は、/etc/default/kbd ファイル (SUN マシン上) で「KEYBOARD_ABORT=disable」という行がコメントになっているか確認してください。この行がコメントになっていない場合、キーボードの中止シーケンスが無効になります。シーケンスを有効にするには、この行をコメント化します。

Dominion KSX II をインストールしたサイトを統合するには、どうすればよいですか。

Raritan の CommandCenter は集中管理を提供するために特別にデザインされています。Dominion KSX II やその他の Raritan ネットワークベース製品などのデバイスの統合管理に注目した場合、優れたソリューションと言えます。

KSX II デバイスの Ethernet ポートは、10/100/1000 Mbps を自動検出しますか。

KSX II には 10/100/1000 Mbps Ethernet インタフェースが 2 個搭載されており、その通信速度と通信方式 (全二重/半二重) を変更できます。通信速度と通信方式は、自動検出に設定するか、または、手動で設定します。

Dominion KSX II は RS422 と RS485 をサポートしますか。

いいえ。現在、Dominion KSX II は非同期 RS232 (一般的にはシリアルと呼ばれます。ただし、シリアルとは RS232 以外にも広く使用される用語です) のみをサポートします。RS422 と RS485 は工業オートメーションおよびその他の市場で使用されます。Dominion KSX II は現在、シリアルで管理されるサーバと、データ センターやサーバ ルームでよく見られるその他のデバイス用に設計されています。これにはシリアルで制御される電源タップ (Raritan のリモート 電源制御デバイスのライン) が含まれます。

KSX II から 300 フィート以上離れたサーバ (シリアルで管理) があります。接続するにはどうすればよいですか。

RS232 から RS422/485 へのサードパーティ製コンバータを、接続先ごと (Dominion 側の端と、デバイスに接続されている端の合計 2 ユニット) に購入する必要があります。

複数のウィンドウを開き、複数のサーバとその他の IT 装置をモニタするために、「並べて表示」することはできますか。

はい。Dominion KSX II にあるシリアル ポートと同じだけウィンドウを「並べて表示」してモニタすることができます。

多数のサーバを管理しています。接続先のサーバはどのように選択すればよいですか。

ブラウザの簡単なメニューで各サーバのユーザ名を割り当てることができます。ユーザはサーバをクリックするだけでポップアップ メニューを開き、コンソール ポートに接続するためメニューから [Connect] (接続) を選択します。SSH/Telnet を使用する場合、ユーザのログオン時、接続が許可されているポートのリストが表示されます。

ユーザが、Dominion KSX II に接続されているすべてのサーバを参照することはできますか。

いいえ。各ユーザは管理/参照が許可されているサーバのリストのみを表示できます。Dominion KSX II の管理者は各サーバにアクセス権限を設定します。

Dominion KSX II は Raritan の CommandCenter™ と併用できますか。

はい、Dominion KSX II は Raritan Command Center™ エンタープライズ規模の管理ソリューションの一部として、展開可能です。数百台におよぶ Dominion KSX II ユニットを CommandCenter で管理できます。

モデムは Dominion KSX II のみを管理するためだけに使用するのですか。

いいえ。このカテゴリに属す他の製品とは異なり、Dominion KSX II は装置の管理だけでなく、ターゲット サーバにアクセスするためにもモデムを使用します。

Dominion KSX II モデルに使用されているモデムは標準のものですか。

はい、内蔵モデムは KSX II モデルの標準です。

sDominion KSX II には接続されたターゲット サーバに対して、どのレベルの制御がありますか。

リモート ユーザは直接コマンド ラインにアクセスでき、メンテナンス、管理、トラブルシューティング、さらに再起動までターゲット デバイスを全体的に制御できます。ユーザの権限は Dominion KSX II のログイン特権とサーバ自体により制限されるのみです。

一部のサーバに接続するためにシリアル アダプタを使用しなければばならないのはなぜですか。

EIA では DB25 と DB9 コネクタの RS232 用に RS232 の標準を公開していますが、RJ45 の RS232 については標準が定められていません。また、一部の製造メーカーでは、EIA が定めた DB25 と DB9 コネクタのピン配列に従っていません。

Dominion KSX II デバイスは、SUN® "ブレークセーフ" ですか。

すべての Dominion KSX II ユニットは SUN Solaris を使用の場合に、SUN「ブレーク セーフ」に対応しています。

Dominion KSX II の管理者パスワードを紛失しました。バックドアや秘密のパスワードはありますか。

バックドア パスワードはありません。唯一の手段は、ユニットを工場出荷時のデフォルト設定に復元し、管理ユーザ名とパスワードを再度作成する方法です。ユニットを工場出荷時のデフォルトに復元するハードウェア リセット機能が備わっています。

KSX II は、どのようなリモート アクセス接続方法に対応していますか。

Dominion KSX II では、複数のリモート アクセス接続方法が可能です。次のような方法があります。インターネット、LAN/WAN、またはダイアルアップ モデム。つまり、サーバはイン バンド、アウト オブ バンドの両方でアクセスすることができ、ネットワークがダウンしても常に基幹ターゲット サーバへのリモート アクセスが可能です。

Dominion KSX II を使用して安全なコンソール セッションを行うために、組織のファイアウォールでどのポートを開いておく必要がありますか。

ポート 443 (HTTPS 用)、ポート 5000 (検出用) およびポート 23 (Telnet 用) (これはオプションでデフォルトでは開きません) になります。オプションで、ユーザ セッション用にポート 80 (HTTP) を開きます。ソフトウェア バージョン 2.2 以降を実行しているユニットの場合はポート 5000 (または 1024-65536 のその他のポート)。ファームウェア 2.2 より前のリリースのソフトウェアを実行している場合は、ポート 23 またはユーザ定義ポート (2000 - 2400)。SSH を使用している場合は、ポート 22 を開く必要があります。

KSX II のオペレーティング システムへはどのようにすればアクセスできますか。

Dominion KSX II は安全なデバイスです。そのため、オペレーティング システムにアクセスすることはできません。

サーバと Dominion KSX II が設置されているラックから離れた場所に、シリアル デバイスを配置しています。これらのデバイスを Raritan スイッチに接続することはできますか。

はい。詳細は、「*シリアル デバイスまでの距離* 『*317*p. の"*シリアル デバイスの距離*"参照先 』」を参照してください。

Dominion KSX II のソフトウェアはどのようにするとアップグレードできますか。

[Firmware Upgrade] (ファームウェアのアップグレード) ページを使用して、KSX II ユニットと接続されているすべての D2CIM-VUSB のファームウェアをアップグレードします。このページは、KSX II リモート コンソールでのみ使用できます。

KSX II ソフトウェアへのアップグレードは無償ですか。

はい。現在、すべてのソフトウェア アップグレードは無償です。

Dominion KSX II では追加のクライアント ソフトウェアが必要ですか。

いいえ。Dominion KSX II はインストールを迅速に、設定を簡単に行うことのできる真の「プラグアンドプレイ」機能を備えています。クライアント ソフトウェアまたはハードウェアを追加購入する必要はありません。また、特別なネットワーク機器またはデザインも不要です。

Dominion KSX II に付属するターミナル エミュレーション パッケージの名前は何ですか。

Raritan シリアル コンソールです。

Dominion KSX II ではどのような認証方式に対応していますか。

ローカル データベース、RADIUS、LDAP/S、Active Directory。

Dominion KSX II では SNMP をサポートしていますか。

はい。Dominion KSX II では Raritan Enterprise MIB を介して、SNMP トラップをサポートします。

Dominion KSX II では Syslog をサポートしていますか。

はい。Dominion KSX II ではプライマリ サーバとセカンダリ サーバで Syslog をサポートします。

サーバとのセッションのキー入力 (ユーザからの入力と、サーバ/デバイスからの応答) すべてをログ記録することはできますか。

はい。KSX II はクライアント側でのログ記録にも対応しています。

Dominion KSX II では Telnet をサポートしていますか。

はい。Dominion KSX II は Dominion KSX II ユニットの Telnet デーモンの有効化をサポートします。Telnet はすべての情報を「平文」で送信するため、Telnet の有効化はお客様のご判断により実行してください。ユニットが工場から出荷される際、デフォルトで Telnet は無効になっています。Raritan では Telnet よりも安全な代替手段として、SSH の使用を強くお勧めします。SSH ではログイン シーケンスを含め、すべてのデータが暗号化されます。

SSH の使用時、SUN™ Solaris™ サーバに対し、意図的な「ブレーク」シグナルを送信することはできますか。

はい。

Web ブラウザの使用時、SUN Solaris サーバに対し、意図的な「ブレーク」シグナルを送信することはできますか。

はい、Raritan シリアル コンソールを使用します。

Telnet の使用時、SUN Solaris サーバに対し、意図的な「ブレーク」シグナルを送信することはできますか。

はい。

SSH の使用時、シリアル ポートからバッファされたオフライン データを取得できますか。

はい。

Telnet の使用時、シリアル ポートからバッファされたオフライン データを取得できますか。

はい。

VPN 接続で KSX II を使用できますか。

はい。KSX II は TCP/IP を使用するほぼすべてのネットワークに対応します。では、レイヤ 1 からレイヤ 4 までの標準的なインターネット プロトコル (IP) 技術が使用されます。VPN (典型的な IPSec) 接続を設定し、Web ブラウザを開始して、Dominion デバイスの URL を入力します。Dominion とのセッションは VPN トンネルを介して、透過的に実行されます。トラフィックは、標準 VPN を介しても容易にトンネル化できます。

Java™ 対応 Web ブラウザの使用時、シリアル ポートからバッファされたオフライン データを取得できますか。

はい。

Dominion KSX II はデータ センターの「クラッシュ カート」アプリケーション用のローカル (ダイレクト) ポート アクセスをサポートしていますか。

はい。

Dominion KSX II シリアル ポートのピン配列は何ですか。

最大のポート密度を提供して簡単な UTP (カテゴリ 5) 配線にするため、KSX II では小型の RJ-45 ポートを介したシリアル接続ができます。ただし、RJ-45 を介したシリアル接続は、業界標準として広く採用されているわけではありません。

RJ-45 コネクタのピン配列を次の表に示します。

RJ-45 ピン	信号
1	RTS
2	DTR
3	TxD

RJ-45 ピン	信号
4	GND
5	DCD
6	RxD
7	DSR
8	CTS

KSX II のシリアル ピン配列（RJ-45）についての最新情報は、Raritan Web サイト（www.raritan.com）のサポート ページを参照してください。

Dominion KSX II はシリアル デバイスへのアクセスに Web ブラウザを使用します。Java 対応 Web ブラウザ アクセスの利点は何ですか。

多くの Solaris/Unix/Linux 管理者の間では、シリアル ホストへのアクセスの事実上の標準は SSH です。しかし、Unix/Linux で使用できる SSH クライアントは Apple Macintosh に対応していません。さらに、Java 対応ブラウザは PDA、およびハンドヘルド PC を含め、多くのプラットフォームで使用できます。Dominion KSX II に備わった簡単な「ポイント アンド クリック」アクセス機能により、管理者は Java 対応 Web ブラウザから安全にアクセスできます。

ユニバーサル仮想メディア

仮想メディアがサポートされている KSX II のモデルはどれですか。

仮想メディアは、すべての KSX II モデルでサポートされています。仮想メディア機能は、KSX II 単体で利用することも、Raritan の集中管理デバイス CC-SG を通じて利用することもできます。

KSX II でサポートされている仮想メディアのタイプはどれですか。

KSX II でサポートされている仮想メディアのタイプは、内蔵または USB 接続された CD/DVD ドライブ、USB 接続された大容量ストレージ デバイス、PC の内蔵ハード ディスク、および ISO イメージです。

仮想メディアに必要なものは何ですか。

KSX II 用の仮想メディア CIM が必要です。このような CIM には、D2CIM-VUSB および新製品である D2CIM-DVUSB の 2 つがあります。

D2CIM-DVUSB には USB コネクタが 2 つあり、仮想メディアを BIOS レベルで利用したいお客様に適しています。D2CIM-DVUSB は、スマート カード認証にも必要です。

D2CIM-VUSB には USB コネクタが 1 つあり、仮想メディアを OS レベルで利用したいお客様に適しています。

どちらの CIM でも、USB 2.0 インタフェースに対応しているターゲット サーバへの仮想メディア セッションがサポートされています。

32 個セットおよび 64 個セットのお得な CIM パッケージが用意されています。これらの CIM でも、ずれないマウスやリモート ファームウェア更新がサポートされています。

仮想メディアは安全ですか。

はい。仮想メディア セッションは、AES または RC4 暗号化方式で保護されます。

USB プロファイル

USB プロファイルとは何ですか。

一部のターゲット サーバでは、仮想メディアなど USB ベースのサービスを利用するために、特別に構成された USB インタフェースを必要とします。USB プロファイルは、KSX II の USB インタフェースをターゲット サーバの特性に合わせて調整するものです。

USB プロファイルを使用するのはなぜですか。

USB プロファイルは、BIOS レベルで特に必要となります。仮想メディア ドライブにアクセスする際、BIOS レベルでは USB 仕様が完全にサポートされていないことがあります。

一方、USB プロファイルはオペレーティング システム レベルで使用されることもあります。たとえば、Mac® サーバや Linux® サーバにおいてマウス動作を同期させる場合などです。

USB プロファイルはどのように使用しますか。

管理者は KSX II の [Port Configuration] (ポート設定) ページで、特定の USB プロファイルを使用するように個々のポートまたはポート グループを設定できます。

必要があれば、USB プロファイルを KSX II クライアントで選択することもできます。

適切な USB プロファイルを選択しなかった場合、どうなりますか。

ターゲット サーバに適した USB プロファイルを選択しなかった場合、大容量ストレージ デバイス、マウス、またはキーボードが適切に動作しなくなるかまたはまったく機能しなくなる可能性があります。

仮想メディアを利用する際、USB プロファイルを必ず設定する必要がありますか。

いいえ。仮想メディアを OS レベルで利用する場合や、仮想メディアにアクセスせずに BIOS レベルで操作する場合、デフォルトの USB プロファイルで十分なケースがほとんどです。

使用可能なプロファイルはどれですか。

「*使用可能な USB プロファイル*『*116*p. の"*使用できる USB プロファイル*"参照 』」を参照してください。

あるターゲット サーバに最適な USB プロファイルを見つけるには、どうすればよいですか。

"Generic" USB プロファイルは、大半のターゲット サーバに最適です。ターゲット サーバに対してこの USB プロファイルが適切に機能しない場合は、「*使用可能な USB プロファイル*『*116*p. の"*使用できる USB プロファイル*"参照 』」で適切な USB プロファイルを探すことができます。ご使用のターゲット サーバに最適な USB プロファイルを選択してください。

BIOS プロファイルの目的は何ですか。

BIOS プロファイルは、USB 仕様を完全に実装していないサーバ BIOS の要件に合わせて調整されたものです。このような USB プロファイルを選択した場合、キーボード、マウス、および仮想メディアを BIOS レベルで使用できるので、BIOS の制約を受けることがありません。

USB プロファイルを使用する際、特別な CIM が必要ですか。

ファームウェアが最新である D2CIM-VUSB または D2CIM-DVUSB を使用する必要があります。

他のターゲット サーバ構成用の USB プロファイルが今後 Raritan から提供される予定がありますか。

Raritan では、お客様のニーズに合わせて新しい USB プロファイルを提供していく予定です。新しい USB プロファイルが提供された場合、ファームウェア アップグレードの中に含まれる予定です。

IPv6 ネットワーキング

IPv6 とは何ですか。

IPv6 は "Internet Protocol Version 6" の頭字語です。IPv6 は次世代の IP プロトコルであり、現在使用されている Internet Protocol Version 4 (IPv4) プロトコルを置き換えるものです。

IPv6 は、IPv4 が抱えているさまざまな問題を解決します (例: IPv4 アドレスの枯渇)。経路選択やネットワーク自動設定などの機能が IPv4 よりも向上しています。IPv6 は徐々に IPv4 を置き換えていくと予想されています。つまり、数年間は両者が共存することになります。

管理者の観点から見ると、IPv6 は IP ネットワークの大きな問題の一つを解消するのに役立ちます。その問題とは、IP ネットワークの設定作業と保守作業です。

KSX II で IPv6 ネットワーキングがサポートされているのはなぜですか。

米国のさまざまな政府機関と国防総省は、調達時に IPv6 対応製品を購入するよう義務付けられています。また、多くの企業および国 (例: 中国) が、今後数年間で IPv6 に移行する予定です。

デュアル スタックとは何ですか。また、デュアル スタックが必要なのはなぜですか。

デュアル スタックは、IPv4 と IPv6 の両方を同時にサポートする機能です。IPv4 から IPv6 に徐々に移行していくことを考えると、デュアル スタックは IPv6 をサポートするうえで必須機能であると言えます。

KSX II 上で IPv6 を有効にするにはどうすればよいですか。

KSX II の [Device Settings] (デバイス設定) メニューの [Network Settings] (ネットワーク設定) をクリックし、[Network Settings] (ネットワーク設定) ページを開きます。次に、[IPv6 Address] (IPv6 アドレス) チェック ボックスをオンにし、[IP Auto Configuration] (IP 自動設定) ボックスの一覧で値を選択します。MPC でも IPv6 を有効にする必要があります。

IPv6 アドレスが設定された外部サーバがあります。この外部サーバを KSX II と併用する場合、どうなるでしょうか。

KSX II から外部サーバ (例: SNMP マネージャ、Syslog サーバ、LDAP サーバ) の IPv6 アドレスを使用してそれらの外部サーバにアクセスすることができます。

具体的に言うと、KSX II のデュアル スタック アーキテクチャを使用することにより、IPv4 アドレス、IPv6 アドレス、またはホスト名を指定してこれらの外部サーバにアクセスすることができます。つまり KSX II は、今後多くのお客様の社内で発生する IPv4/IPv6 混在環境に対応できます。

Dominion KX I で IPv6 はサポートされていますか。

いいえ。Dominion KX I で IPv6 はサポートされていません。

社内ネットワークで IPv6 がサポートされていない場合、どうなるでしょうか。

KSX II は、出荷時設定では IPv4 だけを使用するようになっています。社内ネットワークで IPv6 を使用できる状態になったら、前述の「KSX II 上で IPv6 を有効にするにはどうすればよいですか。」の手順を実行し、IPv6/IPv4 デュアル スタックを有効にします。

IPv6 に関する詳細情報はどこで入手できますか。

www.ipv6.org に、IPv6 に関する全般情報が掲載されています。また、『KSX II User Guide』では KSX II における IPv6 のサポートについて説明されています。

リモート アクセス

各 KSX II からターゲット サーバにリモート アクセスできるユーザは何人ですか。

最大で 8 人の KVM ユーザが 1 つの KVM チャンネルを使用でき、最大 8 人のシリアル ユーザが 8 つのシリアル チャンネルを共有できます。

2 人のユーザが同じターゲット サーバの画面を同時に表示できますか。

確認できます。最大 8 名のユーザが 1 台のサーバに同時にアクセスし、制御できます。

2 人のユーザが同じターゲット サーバにアクセスするとき、一方のユーザがリモートでアクセスし、もう一方のユーザがローカル ポートからアクセスすることはできますか。

可能です。ローカル ポートはリモート "ポート" からは完全に独立しています。PC 共有機能を使用することで、ローカル ポートから同じサーバにアクセスできます。

クライアントから KSX II にアクセスする際、どのようなハードウェア、ソフトウェア、およびネットワーク構成が必要ですか。

KSX II には Web ブラウザを使用してアクセスできるので、クライアント コンピュータにアクセス用のソフトウェアをインストールする必要はありません。ブラウザでの Java 対応は必須ではありません。

KSX II には、主要な Web ブラウザ (Internet Explorer、Mozilla、および Firefox) を使用してアクセスできます。Windows、Linux、Sun Solaris、Macintosh の各デスクトップ コンピュータ上で、Raritan の Java ベースの MPC、RSC、および新しい Virtual KVM Client (VKC) を使用して KSX II にアクセスできるようになりました。

SSH クライアントを使用する場合は、SSH クライアントを用意する必要があります。Linux のような一部のオペレーティング システムでは、SSH クライアントは配布ファイルに含まれています。また、OpenSSH.org でも SSH クライアントを提供しています。

KSX II 管理者は、便利なブラウザ ベースの画面を使用して、リモート管理作業 (例: パスワードとセキュリティの設定、サーバ名の変更、IP アドレスの変更) を行うこともできます。

KSX II にアクセスする際に使用される VKC アプレットのファイル サイズはどのくらいですか。また、この VKC アプレットを取得するのにどのくらいの時間がかかりますか。

KSX II へのアクセスに使用される VKC アプレットのサイズは、約 500 KB です。次の表に、さまざまなネットワーク速度においてこのアプレットを取得するのに要する、おおよその時間を示します。

速度	説明	所要時間
100 Mbps	100 Mbps ネットワークの理論上の速度	0.05 秒
60 Mbps	100 Mbps ネットワークの実効速度	0.08 秒
10 Mbps	10 Mbps ネットワークの理論上の速度	0.4 秒
6 Mbps	10 Mbps ネットワークの実効速度	0.8 秒
512 Kbps	標準的なケーブル モデムのダウンロード速度	8 秒

ネットワークが使用不能になった場合、KSX II に接続されているターゲット サーバにアクセスするにはどうすればよいですか。

KSX II には内蔵モデム ポートが備えられています。このモデムを使用して、ネットワークの障害時にもサーバへリモート アクセスできます。さらに、KSX II のローカル ポートを使用した場合、ネットワークの稼動状態に関係なく、常にラックからターゲット サーバにアクセスできます。

Windows® 以外のクライアントは用意されていますか。

はい。Windows 以外のユーザも、Virtual KVM Client、Raritan シリアル コンソール (RSC)、および Multi-Platform Client (MPC) から KSX II スイッチを使用してターゲット サーバに接続できます。MPC は、Web ブラウザ経由またはスタンドアロンで実行できます。

VKC セッションでときどき Alt キーが受け付けられないようです。どうすればよいですか。

この現象は通常、Alt キーを押したまま離さないときに発生します。たとえば、Alt キーを押しながら Space キーを押し続けると、フォーカスがターゲット サーバからクライアント PC に移ります。続いて、ローカルの OS によってこのキー組み合わせが解析され、このキー組み合わせに対するアクションがクライアント PC のアクティブなウィンドウでトリガされます。

Ethernet と IP ネットワーキング

ProductName< では、冗長フェイルオーバまたは負荷分散を可能にするためにギガビット Ethernet ポートが二重化されていますか。

はい。KSX II では、冗長フェイルオーバを可能にするために Gigabit Ethernet ポートが二重化されています。プライマリ Ethernet ポート（またはそのポートに接続されているスイッチやルータ）に障害が発生した場合、同じ IP アドレスが設定されたセカンダリ Ethernet ポートにフェイルオーバされます。これにより、ターゲット サーバの運用が中断することがなくなります。自動フェイルオーバは、管理者が有効にする必要があります。

ProductName< ではどの程度の帯域幅が必要ですか。

KSX II には、次世代の KVM-over-IP 技術が搭載されています。この技術によって、最高のビデオ圧縮を実現できます。Raritan は、高品質ビデオ伝送と帯域幅節約に関する数多くの技術賞を獲得しています。

Raritan は、ネットワーク帯域幅を節約するためにユーザがビデオ パラメータを調整できる KVM-over-IP 機能を他社に先駆けて開発しました。たとえば、ダイヤルアップ モデム接続で KSX II に接続する場合、ビデオ送信をグレースケールに変更できます。そのため、ユーザはパフォーマンスを維持しつつ効率的に作業できます。

以下のデータに示すのは、その点を考慮した KSX II のデフォルト ビデオ設定です。これらの設定は個別の環境に応じて変更できます。設定値を上げてより高品質なビデオ表示（色深度）を提供したり、設定値を下げて速度の遅い接続用に最適化したりできます。

KSX II のデフォルト設定における帯域幅使用を控えめに見積もると、アクティブな KVM ユーザ（サーバに接続し、サーバを使用しているユーザ）ごとに普通は約 0.5 Mbps となります。一時的に増加した場合、最大で 2 Mbps となります。通常の帯域幅使用はさらに小さいため、値は非常に控えめに見積もられています。

各ビデオ送信で必要な帯域幅は、管理サーバで実行されているタスクによって異なります。画面の変更が多いほど、使用される帯域幅も大きくなります。10 Mbps のネットワークで KSX II をデフォルトに設定した場合の使用例と必要な帯域幅使用について、以下の表にまとめます。

使用例	必要な帯域幅
アイドル状態の Windows デスクトップ	0 Mbps
デスクトップ上でカーソルを移動した場合	0.18 Mbps

使用例	必要な帯域幅
アイドル状態の Windows デスクトップ	0 Mbps
400x600 の静的なウィンドウまたはダイアログ ボックスを動かした場合	0.35 Mbps
スタート メニューを表示した場合	0.49 Mbps
テキストのページ全体をスクロールした場合	1.23 Mbps
3D の迷路のスクリーン セーバを実行した場合	1.55 Mbps

KSX II が動作可能な接続速度の下限値（最低の帯域幅）はどのくらいですか。

ある程度の KSX II のパフォーマンスを実現するには、モデム接続で 33 Kbps 以上の速度が推奨されます。

KSX II の Ethernet インタフェースの速度はどのくらいですか。

KSX II には 10/100/1000 Mbps Ethernet インタフェースが 2 個搭載されており、その通信速度と通信方式（全二重/半二重）を変更できます。通信速度と通信方式は、自動検出に設定するか、または、手動で設定します。

無線接続環境で KSX II にアクセスできますか。

はい。KSX II は、標準の Ethernet を使用するだけでなく、使用帯域幅を抑えつつ高画質を維持する機能を備えています。つまり、クライアントを KSX II に無線で接続している場合、ターゲット サーバを BIOS レベルで設定および管理する作業を無線で行うことができます。

WAN（インターネット）上で、または社内 LAN 上で KSX II を使用できますか。

高速の社内 LAN、速度を予測しにくい WAN（インターネット）、ケーブル モデム接続、ダイヤルアップ モデム接続のいずれの場合でも、KSX II の KVM-over-IP 技術により接続が可能です。

ネットワーク上で KSX II にアクセスできるようにするには、社内ファイアウォールで TCP ポートをいくつ開放する必要がありますか。また、これらのポートは変更できますか。

1 つだけです。KSX II では、TCP ポートを 1 つだけ開放してそのポートにアクセスさせることによって、ネットワーク セキュリティを確保します。このポートは、セキュリティを高めるために変更することもできます。

ただし、KSX II のオプションの Web ブラウザ機能を利用する場合は、標準の HTTPS ポート 443 も開放する必要があります。

KSX II は Citrix 製品と併用できますか。

適切に設定すれば、KSX II を Citrix などのリモート アクセス製品と併用できます。ただし、十分なパフォーマンスが得られるかどうかは保証できません。Citrix のような製品では、デジタル KVM スイッチと概念が似ているビデオ リダイレクト技術が使用されています。したがって、併用した場合 2 種類の KVM-over-IP 技術が同時に使用されることになります。

KSX II を使用するには外部認証サーバが必要ですか。

いいえ。KSX II は完全に自給自足型のデバイスです。IP アドレスを KSX II に割り当てるだけで使用できます。Web ブラウザや認証機能はすべて内蔵されています。

社内で外部認証サーバ（例: LDAP/LDAPS、Active Directory、RADIUS）を使用している場合、KSX II でその外部認証サーバを使用することもできます。また、KSX II で使用している外部認証サーバに障害が発生した場合、KSX II の認証機能にフェイルオーバすることもできます。このように、KSX II の設計理念は、インストール作業を簡素化すること、外部サーバにまったく依存しないようにすること、および、柔軟性を大幅に高めることです。

KSX II で DHCP を使用できますか。

DHCP アドレス割り当ては使用できますが、Raritan では固定 IP アドレスの設定を推奨しています。KSX II はインフラストラクチャ デバイスであるため、固定 IP アドレスを使用した方が、KSX II に対してより効率的にアクセスし、管理できます。

IP ネットワークから KSX II にアクセスできなくなりました。原因は何でしょうか。

KSX II では、お客様の LAN/WAN が使用されます。考えられる原因は次のとおりです。

- Ethernet の自動ネゴシエーション: 一部のネットワークでは、10/100 Mbps の自動ネゴシエーションが適切に機能しません。そのため、KSX II を 100 Mbps/全二重に設定するか、または、そのネットワークに適した値に設定する必要があります。
- IP アドレスの重複: KSX II の IP アドレスが他のデバイスと重複している場合、ネットワーク接続を確立できないことがあります。
- ポート 5000 の競合: 他のデバイスでポート 5000 を使用している場合、そのデバイスと KSX II のいずれかでポートを変更する必要があります。

KSX II の IP アドレスを変更したか、または、新しい KSX II に交換した場合、その IP アドレスと MAC アドレスがレイヤ 2 ネットワークとレイヤ 3 ネットワーク全体に認識されるまで、十分な時間をとる必要があります。

サーバ

KSX II を使用するには Windows® サーバが必要ですか。

いいえ。KSX II は特定のベンダに依存しないデバイスです。Active Directory サーバを使用してユーザを認証するように KSX II が設定されている場合でも、その Active Directory サーバが使用不能になると、KSX II 内部の認証機能がアクティブになるので、認証処理を問題なく続行できます。

KSX II の Web ブラウザ機能を利用する場合、Microsoft® Internet Information Services (IIS) などの Web サーバ ソフトウェアをインストールする必要がありますか。

いいえ。KSX II は完全に自給自足型のデバイスです。KSX II に IP アドレスを割り当てたら、使用可能になります。KSX II には Web ブラウザ機能と認証機能が完全に組み込まれているからです。

ワークステーションから KSX II にアクセスする場合、どのソフトウェアをインストールする必要がありますか。

特別なアクセス用ソフトウェアをインストールする必要はありません。Web ブラウザを使用して KSX II にアクセスし、すべての操作を行うことができます。なお、raritan.com でオプションのクライアント ソフトウェアを入手することもできます。このクライアント ソフトウェアは、モデムを使用して KSX II にアクセスする場合に必要となります。また、Windows を使用していないユーザー向けに、Java ベースのクライアント ソフトウェアが提供されるようになりました。

ブレード サーバ

ブレード サーバを KSX II に接続できますか。

はい。KSX II では、代表的なブレード サーバ メーカ (HP、IBM、および Dell) の主要なブレード サーバ モデルがサポートされています。

サポートされているブレード サーバはどれですか。

サポートされているモデルは次のとおりです。

- Dell® PowerEdge® 1855、1955、および M1000e
- HP BladeSystem c3000 および c7000
- IBM® BladeCenter® H または E

注: IBM BladeCenter Model S、T、および HT にアクセスするには、"IBM (Other)" プロファイルを選択します。

Paragon 用のブレード対応 CIM は使用できますか。

いいえ。Paragon II 用ブレード対応 CIM は KSX II で使用できません。

どの CIM を使用すればよいですか。

使用する CIM は、ご使用のブレード サーバの製造元とモデルにおける KVM ポートのタイプによって決まります。サポートされている CIM は、DCIM-PS2、DCIM-USBG2、D2CIM-VUSB、および D2CIM-DVUSB です。

使用可能なアクセス方法はどれですか。

KSX II にアクセスする方法としては、(1) ローカル ポートからアクセス、(2) IP を使用してリモート アクセス、(3) CC-SG 経由でアクセス、(4) モデムを使用してアクセス、の 4 種類があります。

複数台のブレード サーバを切り替える際、ホットキーを使用する必要がありますか。

一部のブレード サーバでは、複数台のブレード サーバを切り替える際にホットキーを使用する必要があります。ただし、通常はホットキーを使用する必要はありません。ブレード サーバの名前をクリックするだけで、自動的にそのブレード サーバに切り替わります。ホットキーを明示的に使用する必要はありません。

ブレード サーバの管理モジュールにアクセスできますか。

はい。管理モジュールの URL を定義し、KSX II または CC-SG からアクセスすることができます。ワンクリック アクセスが設定されている場合、1 回のクリック操作でアクセスできます。

1 台の KSX II に接続できるブレード サーバは何台ですか。

パフォーマンス上および信頼性上の理由により、1 台の KX II に接続できるブレード サーバ シャーシは、モデルにかかわらず最大 8 台、KSX II の場合は最大 4 台です。

KX II の場合、接続するブレード サーバ シャーシの台数は、デバイスでサポートされているリモート接続数の 2 倍以内にすることを推奨します。たとえば、リモート チャネルが 2 本ある KX2-216 の場合、接続するブレード サーバ筐体を 4 台以内にすることを推奨します。もちろん、残りのサーバ ポートにブレード サーバを接続することもできます。

当社は中小企業であり、KSX II を数台しか使用していません。CC-SG 管理ステーションを使用する必要がありますか。

いいえ、使用する必要はありません。中小企業のお客様は、新しいブレード サーバを利用する際に CC-SG を使用する必要はありません。

当社は大企業であり、CC-SG を使用しています。CC-SG からブレード サーバにアクセスできますか。

はい。KSX II 上でブレード サーバの設定が完了したら、CC-SG から KVM 接続を使用してブレード サーバにアクセスできるようになります。ブレード サーバは、筐体別に CC-SG のカスタム ビューに表示されます。

インバンド KVM アクセスまたは埋め込み KVM アクセスすることはできますか。

はい。ブレード サーバに対するインバンド アクセスおよび埋め込みアクセスは、CC-SG で設定できます。

一部のブレード サーバ上で VMware を実行しています。この構成はサポートされていますか。

はい。CC-SG を使用して、ブレード サーバ上で実行されている仮想マシンを表示し、また、その仮想マシンにアクセスすることができます。

仮想メディアはサポートされていますか。

IBM BladeCenter® Model H または E と D2CIM-DVUSB を併用した構成では、仮想メディアを利用できます。

ずれないマウス機能はサポートされていますか。

ブレード筐体内に KVM スイッチを備えているサーバの場合、通常、ずれないマウス機能はサポートされません。HP 製ブレード サーバおよび一部の Dell 製ブレード サーバの場合、各ブレード サーバに CIM が接続されます。したがって、ブレード サーバ上で実行されている OS でずれないマウス機能がサポートされていれば、そのブレード サーバでずれないマウス機能がサポートされます。

ブレード サーバへのアクセスは安全ですか。

はい。ブレード サーバへのアクセスには、KSX II の標準的なセキュリティ機能（例: 128 ビットまたは 256 ビットの暗号化）がすべての使用されます。その他、ブレード サーバ特有のセキュリティ機能があります。たとえば、ブレード サーバごとにアクセス権限を付与する機能や、入力されたホットキーを拒否する機能などがあるので、不正アクセスの防止に役立ちます。

インストール

KSX II を導入する場合、デバイス本体以外に何を Raritan に注文する必要がありますか。

KSX II に接続するサーバごとに、Dominion CIM、シリアル ケーブル アダプタ、および、サーバのキーボード、ビデオ、マウスのポートに直接接続するアダプタが必要です。

導入時、どのタイプの Cat5 ケーブルを使用すればよいですか。

KSX II に接続するサーバごとに、Dominion CIM、シリアル ケーブル アダプタ、および、サーバのキーボード、ビデオ、マウスのポートに直接接続するアダプタが必要です。

KSX II にはどのようなタイプのサーバを接続できますか。

KSX II は特定のベンダに依存しないデバイスです。標準キーボード ポート、ビデオ ポート、およびマウス ポートを搭載しているあらゆるサーバを接続できます。

サーバを KSX II に接続するにはどうすればよいですか。

「KVM Target サーバへの接続」を参照してください。

サーバは KSX II からどのくらい離すことができますか。

「*シリアル デバイスの距離* 『*317*p. 』」と「*ターゲット サーバとの接続距離および画面解像度* 『*317*p. の"*サポートされているターゲット サーバとビデオ*"参照先 』」を参照してください。

仮想メディア機能とずれないマウス機能をサポートする D2CIM-VUSB および D2CIM-DVUSB の場合は、接続距離を 30 m 以内にすることを推奨します。

一部の OS において、稼動中にキーボードまたはマウスを取り外すとサーバがロックされます。キーボードまたはマウスを取り外したときに、KSX II に接続されているサーバがロックされないようにするには、どうすればよいですか。

Dominion コンピュータ インターフェース モジュール (DCIM) ドングルは、それぞれ接続されているサーバに対する仮想キーボードや仮想マウスとして動作します。この技術は、KME (キーボード/マウス エミュレーション) と呼ばれます。Raritan の KME 技術は、データ センターでの使用に耐えるグレードであり、厳正にテストされています。また、ローエンドの KVM スイッチの技術に比べてはるかに高い信頼性が確保されています。この技術には 15 年間以上に及ぶ実績も生かされており、世界中で何百万台ものサーバに実装されています。

KSX II に接続するサーバに何らかのエージェント ソフトウェアをインストールする必要がありますか。

KSX II に接続するサーバにエージェント ソフトウェアをインストールする必要はありません。KSX II はハードウェアを介してサーバのキーボード ポート、ビデオ ポート、およびマウス ポートに直接接続するからです。

それぞれの KSX II に何台のサーバを接続できますか。

KSX II モデルは、4 から 8 台のサーバ ポートで 1U シャーシごとに構成されます。このポート密度は、デジタル KVM スイッチ分野で業界最高水準です。

ある KSX II からサーバを切断し、別の KSX II に再接続するかまたは同じ KSX II の別のポートに再接続した場合、どうなりますか。

サーバ接続先ポートを変更した場合、サーバ ポート名が自動更新されます。この変更内容は、ローカル クライアントおよびすべてのリモート クライアントに反映されます。CC-SG を使用している場合は、CC-SG にも反映されます。

シリアルと KVM の両方のポートも問題なく移動できます。ただし、いったん切断すると、KVM の名前は残りますが、シリアル ポートの名前は残りません。

ローカル ポート

ラックからサーバに直接アクセスできますか。

はい。ラックでは、KSX II は従来型 KVM スイッチと同じように機能します。つまり、1 組のキーボード、モニタ、およびマウスを使用して、最大 16 台のサーバを制御できます。

自分がローカル ポートを使用しているとき、他ユーザがサーバにリモート アクセスできないように設定できますか。

いいえ。KSX II のローカル ポートにおけるサーバへのアクセス パスは、ローカル ポート専用です。したがってユーザは、ラックからサーバにローカル アクセスする際、同時にリモート アクセスするユーザの数を制限する必要はありません。

USB キーボードまたは USB マウスをローカル ポートで使用できますか。

はい。KSX II のローカル ポート エリアには 3 つの USB ポートがあります。USB ポートは USB v1.1 対応であり、キーボードとマウスしか接続できません。スキャナやプリンタなどの USB デバイスは接続できません。

ローカル アクセスする場合、OSD 表示されますか。

はい。ただし、KSX II へのローカル アクセスは、従来の Onscreen Display (OSD) よりもはるかに優れています。KSX II では、ローカル アクセス用に業界初の Web ブラウザ画面が用意されており、また、ローカル アクセスとリモート アクセスの両方に対して同じ画面がが使用されます。さらに、大半の管理機能をローカルで実行できます。

ローカル ポートを使用しているとき、サーバを切り替えるにはどうすればよいですか。

ローカル ポートを使用しているとき、接続されているサーバが、リモート クライアントと同じ画面に表示されます。サーバを切り替えるには、切り替え先サーバをマウスでクリックします。

承認されたユーザだけがローカル ポートからサーバにアクセスできるようにするには、どうすればよいですか。

ユーザがローカル ポートを使用するには、リモートでアクセスする場合と同レベルの認証を受ける必要があります。これは次のことを意味します。

- KSX II が外部の認証サーバ (RADIUS サーバ、LDAP/LDAPS サーバ、または Active Directory サーバ) と連係するように設定されている場合、ユーザがローカル ポートを使用しようとしたときに、リモート ユーザと同じサーバで認証されます。
- 外部の認証サーバが使用不能になった場合は、KSX II 内部の認証データベースにフェイルオーバされます。

KSX II 自体に認証機能が備わっているので、設置後すぐに使用を開始できます。

ローカル ポートを使用して、接続されているサーバの名前を変更した場合、この変更内容はリモート クライアントにも反映されますか。また、CC-SG を使用している場合、この変更内容が CC-SG にも反映されますか。

はい。ローカル クライアント、リモート クライアント、および CC-SG における画面表示内容は同一であり、完全に同期しています。つまり、KSX II の OSD でサーバの名前を変更すると、この変更内容がすべてのリモート クライアントおよび外部の管理サーバにリアルタイムで反映されます。

KSX II のリモート管理ツールを使用して、接続されているサーバの名前を変更した場合、その変更内容がローカル クライアントにも反映されますか。

はい。ローカル ポートの表示は、まったく同じで、リモート アクセス クライアントと完全に同期されています。つまり、KSX II のオンスクリーン表示でサーバの名前を変更すると、すべてのリモート クライアントと外部管理サーバがリアルタイムで更新されます。

ローカル クライアントの画面に影のようなものが発生することがあります。これはなぜですか。

LCD モニタを長時間使用すると、このような影や残像が発生する可能性があります。画面を長時間表示し続けると、LCD の特性と帯電が原因でこのような影が発生することがあります。

電源制御

KSX II で使用する電源では、電圧設定が自動検出されますか。

はい。KSX II の電源は、100 ～ 240 V、50 ～ 60 Hz の範囲の AC 電圧で使用できます。

KSX II の電源制御機能はどのタイプですか。

Raritan の Remote Power Control (RPC) 電源タップを KSX II に接続することにより、KVM ターゲット サーバの電源を制御できます。簡単な設定作業を 1 度行えば、その後はサーバ名を右クリックするだけで、サーバの電源を投入または切断すること、および、ハングしたサーバの電源を再投入することができます。電源再投入は、サーバの AC 電源コードをいったん抜いて再度差し込むことと同じです。

KSX II では、電源を複数個備えたサーバはサポートされていますか。電源がそれぞれ別のラック PDU (電源タップ) に接続されている場合はどうなりますか。

はい。複数台の電源を別々の電源タップに接続する構成をサポートするように、KSX II を設定できます。KSX II デバイスには最大 2 個の電源タップを接続できます。ターゲット サーバごとに 4 台の電源を、別々の電源タップに接続できます。

電源をリモート制御する場合、特別なサーバ構成にする必要がありますか。

一部のサーバでは、電源をいったん切断して再投入したときにサーバが自動再起動しないように、BIOS が設定されています。このようなサーバを使用する場合、そのサーバのドキュメントを読み、この設定を変更してください。

KSX II でサポートされているラック PDU (電源タップ) のタイプはどれですか。

KSX II の電源制御画面、および、重要なセキュリティ機能を利用するには、Raritan の Remote Power Control (RPC) 電源タップまたは Dominion PX 電源タップを使用します。KSX II の PDU ポートを PX または RPC ユニットに接続するには、CAT5 ケーブルを使用します。

Dominion PX はインテリジェントな電源タップで、Raritan KVM スイッチやセキュア コンソール サーバを介して、リモート サーバやその他のネットワーク デバイスの再起動、データ センターでの電源のモニタなどを実行できます。

拡張性

複数台の KSX II を接続して 1 つのソリューションとして使用するには、どうすればよいですか。

複数台の KSX II を物理的に相互接続する必要はありません。代わりに、各 KSX II をネットワークに接続します。Raritan の CC-SG 管理デバイスを使用して KSX II を配備した場合、KSX II 同士が自動的に連係動作し、1 つのソリューションとして機能します。CC-SG は、リモート アクセスおよびリモート管理用の単一のアクセス ポイントとして機能します。たとえば、設定作業を集中管理すること、ファームウェア更新作業を集中管理すること、認証データベースを一本化することなどができるので便利です。

また、CC-SG を使用することにより、高度な方法でサーバを分類することやアクセス権限を付与することができます。CC-SG を配備できない場合でも、KSX II どうしが自動的に連係動作するので、拡張性が向上します。KSX II のリモート ユーザ インタフェースおよび MPC では、KSX II が自動検出されます。検出されなかった KSX II にアクセスするには、ユーザが作成したプロファイルを使用します。

現在使用しているアナログ KVM スイッチを KSX II に接続できますか。

はい。アナログ KVM スイッチを KSX II のいずれかのサーバ ポートに接続できます。具体的には、D2CIM-DVUSB または D2CIM-VUSB を使用して、現在使用しているアナログ KVM スイッチのユーザ ポートに接続します。アナログ KVM スイッチの仕様はそれぞれ異なっているため、Raritan では、サードパーティ製アナログ KVM スイッチとの相互運用性については保証していません。詳細については、Raritan のテクニカル サポート部門にお問い合わせください。

セキュリティ

KSX II は FIPS 140-2 に対応していますか。

KX II 2.2.0 以降と KSX II 2.3.0 には、FIPS 140-2 の実装ガイドラインに従って、Linux プラットフォームで実行されている FIPS 140-2 で検証された埋め込み暗号化モジュールを使用するためのオプションが用意されています。ビデオ、キーボード、マウス、仮想メディア、およびスマート カードのデータで構成される KVM セッション トラフィックの暗号化には、この暗号化モジュールが使用されます。

KSX II で使用されている暗号化方式は何ですか。

KSX II では、SSL 通信とデータ ストリームの両方において、業界標準である極めて安全な 128 ビット RC4、128 ビット AES、または 256 ビット AES 暗号が使用されます。実際に、暗号化によってセキュリティが確保されていないリモート クライアントと KSX II の間では、データは送信されません。

KSX II では、米国政府の NIST および FIPS で推奨されている AES 暗号がサポートされていますか。

KSX II では、セキュリティを高めるために Advanced Encryption Standard (AES) が使用されます。

AES は米国政府の承認した暗号アルゴリズムです。NIST (米国の国立標準技術研究所) の FIPS 標準 197 で推奨されています。

KSX II ではビデオ データを暗号化できますか。それとも、キーボード データとマウス データだけが暗号化されますか。

競合製品ではキーボード データとマウス データだけが暗号化されますが、KSX II ではセキュリティに関して妥協していません。KSX II では、キーボード データ、マウス データ、およびビデオ データをすべて暗号化できます。

KSX II は外部認証サーバ (例: Active Directory® サーバ、RADIUS サーバ、LDAP/S サーバ) とどのように連係動作しますか。

KSX II では、非常に簡単な設定で、すべての認証要求を LDAP/S、Active Directory、RADIUS などの外部サーバに転送するよう指定できます。また、ユーザが認証されるたびに、そのユーザが所属するユーザ グループに関する情報が、外部認証サーバから KSX II に送信されます。KSX II では、そのユーザが所属するユーザ グループに基づいて、そのユーザに付与するアクセス権限が決まります。

ユーザ名とパスワードはどのように保存されますか。

KSX II の内部認証機能を使用する場合、ユーザ名やパスワードなどの機密情報はすべて暗号化されたうえで保存されます。実際に、Raritan のテクニカル サポートやプロダクト エンジニアリング部門を含め、誰もこれらのユーザー名やパスワードを読み出せません。

KSX II では強力なパスワードを使用できますか。

はい。KSX II には、管理者が設定できる強力パスワード検査機能が備わっています。この機能により、ユーザが作成したパスワードが社内および政府の基準を満たしているかどうか、および、ブルート フォース（総当たり）攻撃によって解読されにくいかどうかが検査されます。

KSX II で [Encryption Mode]（暗号化モード）を [Auto]（自動）に設定した場合、どのレベルの暗号化が行われますか。

KSX II は AES-256 をサポートするための機能を備えています。このため、Java の無制限強度ポリシー ファイルをクライアント コンピュータに読み込む必要があります。一度有効にすると、モードが [AUTO]（自動）に設定された場合、自動的に設定される暗号化レベルは次のとおりです。

ブラウザ	暗号化レベル
Internet Explorer 6、7、および 8	[AES-128]
Firefox 1.5、2.0 3.x	[AES-256]
Safari 2.0.4	[AES-256]

KSX II ではセキュリティ バナーをカスタマイズできますか。

はい。政府機関や軍のようなセキュリティを重視するお客様では、ユーザがログインする前にセキュリティ メッセージを表示する必要があります。KSX II では、カスタマイズ可能なバナー メッセージを表示できます。また、このメッセージへの同意を義務付けることもできます。

スマート カード認証と CAC 認証

KSX II では、スマート カード認証と CAC 認証はサポートされていますか。

はい。KX II 2.1.10 以降および KX II 2.3.0 以降では、ターゲット サーバへのスマート カード認証と DoD Common Access Card (CAC) 認証がサポートされています。

スマート カードと CAC がサポートされている KSX II のモデルはどれですか。

すべての KSX II モデルでサポートされています。Dominion KX II-101 では、現在スマート カードと CAC はサポートされていません。

大企業や中小企業でもスマート カードは使用されていますか。

はい。なお、スマート カードを最も積極的に導入しているのは米国連邦政府です。

スマート カードと CAC がサポートされている CIM はどれですか。

D2CIM-DVUSB が必要です。この CIM をリリース 2.1.10 以降および KSX II 2.3.0 以降のファームウェアでアップグレードする必要があります。

必要なファームウェア バージョンは何ですか。

KX II リリース 2.1.10 以降、または KSX II 2.3.0 以降が必要です。

サポートされているスマート カード リーダーはどれですか。

必要なリーダー標準は、USB CCID と PC/SC です。「*サポートされているスマート カード リーダーとサポートされていないスマート カード リーダー* 『*310*p. 』」を参照してください。

スマート カード/CAC 認証は、ローカル ポートおよび CommandCenter で使用できますか。

はい。ローカル ポートを使用する場合、互換性のあるスマート カード リーダーを KSX II の USB ポートに接続します。

Paragon のスマート カードに対応した UST および CIM は使用されていますか。

いいえ。P2-EUST/C および P2CIM-AUSB-C は、KSX II ソリューションに含まれていません。

管理機能

Web ブラウザを使用して KSX II をリモートで管理および設定できますか。

はい。Web ブラウザを使用して、KSX II のすべての設定をリモートで行うことができます。ただし、リモート クライアントに適切なバージョンの Java Runtime Environment (JRE) がインストールされている必要があります。

KSX II の IP アドレスを初期設定できるだけでなく、KSX II に関するすべての情報をネットワーク上で設定できます。Ethernet クロス ケーブルと KSX II のデフォルト IP アドレスを使用することにより、Web ブラウザから出荷時の初期設定値を変更することができます。

KSX II の設定情報をバックアップおよび復元できますか。

はい。KSX II のデバイス設定情報とユーザ設定情報はすべてバックアップできるので、大規模障害が発生した場合でも復元できます。

KSX II のバックアップ/復元処理は、ProductName リモート コンソールを使用して、ネットワーク経由でリモートで行うこともできます。

KSX II ではどのような監査処理およびログ記録処理が実行されますか。

アカウンタビリティの観点から、KSX II では主要なユーザ イベントとシステム イベントがタイムスタンプ付きでログ記録されます。記録されるイベントの例としては、ユーザのログオン、ユーザのログオフ、特定サーバへのユーザ アクセス、失敗したログオン、設定変更などがあります。

KSX II と Syslog は一元化できますか。

はい。KSX II には、内部にログを記録する機能が備わっていますが、それに加えて、ログ記録されたすべてのイベントを中央の Syslog サーバに送信することもできます。

KSX II と SNMP は一元化できますか。

はい。KSX II には、内部にログを記録する機能が備わっていますが、それに加えて、SNMP トラップを SNMP マネージャ (例: HP OpenView、Raritan の CommandCenter NOC (CC-NOC)) に送信することもできます。

KSX II の内部クロックを時刻サーバと同期させることができますか。

はい。KSX II では業界標準の NTP プロトコルがサポートされているので、内部クロックを社内または社外の時刻サーバと同期させることができます。なお、社外の時刻サーバと同期させるには、KSX II から送信される NTP 要求が社内ファイアウォールを通過できる必要があります。

その他

KSX II のデフォルトの IP アドレスは何ですか。

192.168.0.192

KSX II のデフォルトのユーザ名とパスワードは何ですか。

KSX II のデフォルトのユーザ名は admin、デフォルトのパスワードは raritan です (すべて小文字)。ただし最高レベルのセキュリティを確保するため、KSX II の初回起動時に、デフォルトの管理者ユーザ名と管理者パスワードを変更するよう要求されます。

KSX II の管理者パスワードを変更しましたが、変更後のパスワードを忘れてしまいました。新しいパスワードを発行してもらえますか。

KSX II のハードウェア リセット ボタンを押すと、ProductName が出荷時設定にリセットされます。このとき、管理者パスワードも出荷時設定にリセットされます。

Firefox® を使用して KSX II にログオンした後、別の Firefox ブラウザを開きました。この場合、2 番目に開いた Firefox ブラウザから同じ KSX II に自動ログオンされます。これは問題ないのでしょうか?

問題ありません。ブラウザとクッキーが機能している証拠です。

Firefox を使用して KSX II にログオンした後、同じクライアント コンピュータから別の Firefox ブラウザ セッションを使用して別の KSX II にログオンしようとしました。すると、両方の KSX II からログオフされました。これは正常な動作ですか。

はい。別の KSX II にアクセスするには、最初のセッションを切断するか、または、別のクライアント コンピュータを使用してください。

索引

[

[Audit Log] (監査ログ) - 228, 280, 282
[Authentication Settings] (認証設定) - 134
[Auto-sense Video Settings] (ビデオ設定の自動検出) - 74
[Connection Properties] (接続プロパティ) - 67
[Device Information] (デバイス情報) - 229
[Device Services] (デバイス サービス) - 4, 153
[Encryption & Share] (暗号化および共有) - 4, 213, 218, 282
[Event Management - Destinations] (イベント管理 - 送信先) の設定 - 165
[Event Management Settings] (イベント管理設定) の設定 - 163, 165
[Keyboard Macros] (キーボード マクロ) - 70
[KSX II Diagnostics] (KSX II 診断) ページ - 246
[Local Drives] (ローカル ドライブ) - 111
[Login Limitations] (ログイン制限) - 207, 208
[Network Interface] (ネットワーク インタフェース) ページ - 242
[Network Statistics] (ネットワーク統計) ページ - 243
[Ping Host] (ホストに ping する) ページ - 245
[Port Access] (ポート アクセス) ページ - 4, 51
[Port Access] (ポート アクセス) ページ (ローカル コンソール サーバ ディスプレイ) - 270
[Port Action] (ポート アクション) メニュー - 52, 53, 271
[Strong Passwords] (強力なパスワード) - 146, 207, 210
[Trace Route to Host (ホストへのルートの追跡)] ページ - 245
[Upgrade History] (アップグレード履歴) - 238
[Upgrading Firmware] (ファームウェアのアップグレード) - 235
[USB Profile Management] (USB プロファイルの管理) - 233, 234
[お気に入りの管理] ページ - 56
[お気に入りリスト] ページ - 57, 58
[ユーザ ブロック] - 207, 211

A

A. AC 電源: - 29
Active KVM Client (AKC) - 4, 45, 91
AES (256 ビット) を使用する際の前提条件と Java のサポート対象構成 - 332
AKC ダウンロード サーバ証明書の検証の有効化 - 92, 159
AKC でサポートされている .NET Framework、オペレーティング システムとブラウザ - 92
AKC を使用するための必要条件 - 93
Apple Macintosh の設定 - 27

B

B. ネットワーク ポート - 30

C

C. ローカル ユーザ ポート (ローカル PC) およびローカル管理ポート - 30
CC Unmanage - 239
CC-SG に関する留意事項 - 345
CC-SG ユーザへの注意事項 - 41, 42
CC-SG 管理の終了 - 240
CD-ROM/DVD-ROM/ISO イメージ - 108, 113
CIM アップグレード - 116, 234
CIM キーボード/マウス オプションの設定 - 73
CIM に関する留意事項 - 344
CIM の互換性 - 116
CLI コマンド - 250, 258
CLI の画面操作 - 254, 255
CLI プロンプト - 258
CLI を使用したポート共有 - 260
CLI を使用した初期設定 - 257
CLI を使用しての KSX II へのアクセス - 251
CLI 構文
　ヒントとショートカット キー - 256
connect コマンド - 262

D

D. KVM ターゲット サーバ ポート - 31

DB25F Null 化シリアルアダプタのピン配列 - 322
DB25M Null 化シリアルアダプタのピン配列 - 322
DB9F Null 化シリアルアダプタのピン配列 - 321
DB9M Null 化シリアルアダプタのピン配列 - 321
Dell OptiPlex および Dimension コンピュータ - 344
Dell ブレード シャーシの設定 - 178
Dell 筐体を接続する場合のケーブル長と画面解像度 - 176, 178, 183, 339

E

E. ラック PDU (電源タップ) - 32, 171
Ethernet と IP ネットワーキング - 362

F

F. シリアル ターゲット ポート - 33
FAQ - 346
Fedora Core のフォーカスに関する問題を解決する - 340
Fedora サーバへの VKC および MPC のスマート カード接続 - 341
Fedora 使用時の Firefox のフリーズに関する問題の解決 - 341
FIPS 140-2 サポートの要件 - 218
FIPS 140-2 の有効化 - 215, 217

H

HP および Cisco UCS のブレード シャーシ設定 (ポート グループ管理) - 190, 192, 206
HTTP ポートおよび HTTPS ポートの設定 - 4, 154, 309

I

IBM AIX 5.3 の設定 - 27
IBM ブレード シャーシの設定 - 183
interface コマンド - 261
IP アクセス制御を設定する - 219
IP アドレスの割り当て - 36
ipv6 コマンド - 263
IPv6 ネットワーキング - 358

J

Java - 332
Java Runtime Environment (JRE) - 333

K

KSX II - KSX II 構成の Paragon CIM に関するガイドライン - 304
KSX II - Paragon II 構成に関するガイドライン - 305
KSX II インタフェース - 48
KSX II からのユーザのログオフ (強制ログオフ) - 5, 134
KSX II コンソール サーバ設定用コマンドを使用する - 260
KSX II サブネット上のデバイスの検出 - 58
KSX II のクライアント アプリケーション - 6
KSX II のシリアル RJ-45 ピン配列 - 320
KSX II のローカル ポートの設定 - 201
KSX II の概要 - 2
KSX II の再起動 - 238
KSX II への SSH 接続 - 251
KSX II への Telnet 接続 - 252
KSX II へのローカル シリアル ポート接続 - 253
KSX II ヘルプ - 5
KSX II ユーザ リストの表示 - 132
KSX II リモート コンソール インタフェース - 45, 46
KSX II リモート コンソールの起動 - 46
KSX II ローカル コンソール - 264
KSX II デバイス - 45
KSX II ローカル コンソール インタフェース - 265
KSX II ローカル コンソールでサポートされる言語 - 308
KSX II ローカル コンソールの [Factory Reset] (出荷時設定にリセット) ページ - 280
KSX II ローカル コンソールの [Local Port Settings] (ローカル ポート設定) ページ - 277
KSX II ローカル コンソールの画面に切り替える - 277
KSX II ローカル コンソールを使用する - 265
KVM ターゲット サーバの切り替え - 64

KVM ターゲット サーバの切断 - 66
KVM ターゲット サーバへの接続 - 61, 66
KVM プロパティ - 315
KVM ポート用のプロファイルの選択 - 123

L

LAN インタフェース設定 - 38, 147, 151, 152
LDAP/LDAPS から返す場合 - 324
LDAP/LDAPS スキーマの更新 - 324
LDAP/LDAPS リモート認証の実装 - 134, 135
Linux ターゲット サーバに対して Windows の 3 ボタン マウスを使用する場合 - 344
Linux の設定の永続化 - 23
Linux 設定 (標準マウス モードの場合) - 21

M

Mac のブート メニュー使用時のマウス モード - 120, 123, 199
Macintosh キーボード - 339
Microsoft Active Directory から返す場合 - 325
Microsoft Active Directory についての注意事項 - 42
MPC、VKC、および AKC と組み合わせて使用する場合のプロキシ サーバ設定 - 59
Multi-Platform Client (MPC) - 45, 94

N

name コマンド - 262

P

PX への名前の割り当て - 172

R

RADIUS リモート認証の実装 - 135, 140
RADIUS 通信交換仕様 - 143
Raritan Serial Console (RSC) - 45, 95
Raritan Virtual KVM Client について - 61

S

SSH を有効にする - 154
SSL 証明書 - 221
Sun Solaris の設定 - 24
Sun サーバへのアクセス時に使用できる特別なキー組み合わせ - 276
SUSE Linux 10.1 の設定 - 22
SUSE と VESA のビデオ モード - 343

T

Telnet 接続を有効にする - 153, 252
Telnet、IP アドレス、または SSH 経由のダイレクト ポート アクセスの構成 - 39, 157

U

UNIX の設定の永続化 - 23
UNIX、Linux、および MPC 向け認定モデム - 283
UNIX/Linux ワークステーションからの SSH アクセス - 252
URL を経由したダイレクト ポート アクセスの有効化 - 39, 92, 156, 157
USB プロファイル - 4, 67, 115, 199, 356
USB プロファイルの設定 ([Port] (ポート) ページ) - 123, 186, 199
USB プロファイルの選択 - 66
USB プロファイルの選択に関するヘルプ - 341
USB ポートおよびプロファイルに関する留意事項 - 341
User Management - 124

V

Virtual KVM Client (VKC) - 45, 53, 61, 92, 108, 115
VKC のバージョンが CC-SG プロキシ モードで認識されない - 345
VKC 仮想メディア - 83
VM-CIM および DL360 の USB ポート - 341

W

Web ブラウザ インタフェースの追加に関するヒント - 178, 181, 183, 186, 188
Web ブラウザからの MPC の起動 - 94
Windows 2000 のダイヤルアップ ネットワーク設定 - 285
Windows 2000 の仮想メディアへのアクセス - 344
Windows 2000 の設定 - 20
Windows 7 および Windows Vista の設定 - 19
Windows PC から Telnet で接続する - 252

Windows PC からの SSH アクセス - 251
Windows Vista のダイヤルアップ ネットワーク設定 - 289
Windows XP のダイヤルアップ ネットワーク設定 - 290
Windows XP、Windows 2003、および Windows 2008 の設定 - 18
Windows 環境での VKC および AKC を介した仮想メディア - 106

あ

アメリカ英語以外のキーボード - 336
イベント管理 - 162
インストール - 369
インストールと設定 - 16
インタフェース - 44
インタフェースおよび画面操作 - 48
インテリジェント マウス モード - 17, 81
オペレーティング システムの IPv6 のサポートに関する留意事項 - 335
オペレーティング システムのマウスとビデオの設定 - 18
お気に入りの管理 - 50, 55
お気に入りの追加、削除、および編集 - 58

か

キーボード - 336
キーボード マクロの作成 - 70
キーボード マクロの実行 - 73
キーボード マクロの変更および削除 - 73
キーボード レイアウト コードの変更 (Sun ターゲット) - 43
キーボードのオプション - 70
キーボード言語の設定 (Fedora クライアント) - 337
クライアント ダイヤルアップ ネットワーク設定 - 285
グループベースの IP ACL (アクセス制御リスト) - 126, 129
コマンド ライン インタフェース (CLI) - 45, 249
コマンドのオート コンプリート - 255
コンセントの電源オン/オフの切り替えまたは電源再投入を行う - 98
コンセントへの KVM およびシリアル ターゲット サーバの関連付け ([Port] (ポート) ページ) - 172
コンピュータ インタフェース モジュール (CIM) - 116, 302
ご使用のブラウザで AES 暗号化方式がサポートされているかどうかを確認する - 214, 216

さ

サーバ - 366
サーバ表示 - 272
サポートされている Paragon II CIMS および設定 - 4, 216, 303
サポートされているオペレーティング システム (クライアント) - 4, 298
サポートされているオペレーティング システムおよび CIM (KVM ターゲット サーバ) - 4, 31, 299, 348
サポートされているスマート カード リーダーとサポートされていないスマート カード リーダー - 84, 267, 310, 377
サポートされているターゲット サーバとビデオ - 317, 369
サポートされているブラウザ - 302
サポートされているブレード シャーシ モデル - 192
サポートされているプロトコル - 42
サポートされているリモート接続 - 315
サポートされている画面解像度 - 4, 22, 27, 307, 317
シリアル アクセス - 349
シリアル コンソール アクセスを有効にする - 155
シリアル デバイスの距離 - 317, 352, 369
シングル マウス モード - 83
CC-SG の管理下にあるターゲットに接続する場合 - 345
スキーマ キャッシュを更新する - 328
スキーマへの書き込み操作を許可するようにレジストリを設定する - 325
ステップ 2
ネットワーク ファイアウォールの設定 - 16, 28
ステップ 3

装置の接続 - 11, 16, 29
すべての CLI レベルで使用できるコマンド - 256
スマート カード - 4, 84
スマート カード リーダー - 4, 310
スマート カード リーダー使用時の USB プロファイルの変更 - 343
スマート カードの最小システム要件 - 267, 311
スマート カード認証と CAC 認証 - 377
ずれないマウス モード - 82
セキュリティ - 375
セキュリティ バナー - 4, 224
セキュリティと認証 - 266
セキュリティの管理 - 207
セキュリティの設定 - 104, 107, 132, 207
セキュリティ上の問題 - 259
その他 - 379
ソフトウェア - 9

た

ターゲット コマンドによるスクリーンショット (ターゲット スクリーンショット) - 77
ターゲット サーバにアクセスする - 276
ターゲット サーバの使用 - 6, 44
ターゲット サーバの電源管理 - 65
ターゲット サーバの命名 - 38
ターゲット サーバの要件 - 312
ターゲットでのエミュレーションの設定 - 259
ターゲットの設定 - 173
ターゲット接続と CLI - 259
ツール オプション - 87
ツール バーのボタンおよびステータス バーのアイコン - 62
デスクトップの背景 - 17
デバイスのポート間の移動 - 345
デバイス管理 - 147
デフォルト パスワードの変更 - 35
デフォルトのログイン情報 - 16

な

ネットワーク パラメータの設定 - 257
ネットワークを設定する - 260
ネットワーク基本設定 - 147, 148
ネットワーク設定 - 29, 36, 38, 147, 148, 151, 309, 315
ネットワーク速度の設定 - 152, 318

は

バージョン情報 - Virtual KVM Client - 91
ハードウェア - 8
はじめに - 1
パスワードの変更 - 146
バックアップと復元 - 190, 230
パッケージの内容 - 14
パラメータ値を設定する - 257
ビデオのプロパティ - 74
ビデオ設定の調整 - 75
ファイル追加後に仮想メディアが最新の情報に更新されない - 344
ブラウザに関する留意事項 - 340
フランス語キーボード - 336
ブレード サーバ - 366
ブレード シャーシでサポートされている CIM - 193
ブレード シャーシのサンプル URL フォーマット - 182, 198
ブレード シャーシの設定 - 174
ブレード シャーシの必須および推奨設定 - 176, 178, 183, 196
プロファイル名の競合を処理する - 234
ヘルプでの最新情報 - 4
ポート キーワード - 204
ポート グループ管理 - 206
ポートの設定 - 169
ポート権限 - 126, 128
ポート設定 - 253
ホット キーと接続キー - 273

ま

マウス オプション - 78
マウス ポインタの同期 - 79
マウス ポインタの同期 (Fedora) - 340
マウスの設定 - 17
メンテナンス機能 (ローカル/リモート コンソール) - 227
モデムを設定する - 160
モデム設定 - 11, 283

や

ユーザ - 132
ユーザ グループ - 124
ユーザ グループ リスト - 125
ユーザ グループおよびユーザを作成する - 42
ユーザ グループ情報を Active Directory サーバから返す - 139
ユーザ グループ情報を RADIUS 経由で返す - 143
ユーザ グループ情報を返す - 324
ユーザ メンバの rciusergroup 属性を編集する - 329
ユーザが同時接続可能 - 265
ユーザとグループの関係 - 125
ユーザ認証プロセス - 145
ユニバーサル仮想メディア - 355

ら

ラック PDU (電源タップ) のコンセントの制御 - 97
リセット ボタンを使用して KSX II をリセットする - 11, 282
リモート アクセス - 360
リモート クライアントの要件 - 313
リモート コンソールから RSC を開く - 95
リモート認証 - 42, 203, 279
ローカル コンソールの USB プロファイル オプション - 268
ローカル コンソールのスマート カード アクセス - 86, 267
ローカル サブネット上のデバイスの検出 - 57
ローカル ポート - 371
ローカル ポートの管理 - 277
ローカル ポートの要件 - 311
ログアウト - 59
ログオン - 253

漢字

仮想メディア - 6, 83, 100
仮想メディア ファイル サーバのセットアップ (ファイル サーバ ISO イメージの場合のみ) - 108, 109
仮想メディアに関する留意事項 - 344
仮想メディアの使用 - 107
仮想メディアの切断 - 109, 114
仮想メディアへの接続 - 111
仮想メディアを使用するための条件 - 104, 107
仮想メディア機能利用時におけるターゲット サーバの BIOS の起動時間 - 344
画面を更新する - 74
外部製品の概要 - 9
概要 - 16, 92, 97, 101, 115, 250, 264, 332
各言語に対して KSX II でサポートされているキーボード - 274
拡張性 - 374
環境要件 - 313
管理機能 - 378
関連文書 - 5
既存のユーザ グループの変更 - 131, 133
緊急時の接続 - 314
検出ポートを入力する - 155
権限 - 126, 127
個別グループの許可の設定 - 127, 133
高速の仮想メディア接続を使用した場合の仮想メディアの接続エラー - 345
左パネル - 49
最大垂直走査周波数の変更 - 78
仕様 - 31, 297
使用される TCP ポートおよび UDP ポート - 308
使用されるポート - 315
使用できる USB プロファイル - 116, 342, 356
手順 1
KVM ターゲット サーバの設定 - 16, 17
手順 4
KSX II の設定 - 16, 35
手順 6
キーボード言語の設定 (オプション) - 16, 43
色の調整 - 75
新しい属性を作成する - 326
新規ユーザ グループの追加 - 126, 132
新規ユーザの追加 - 132
診断 - 242
製品の写真 - 7

製品の特長 - 8
接続 - 314, 319
接続キーの例 - 202, 273
接続情報 - 69
全般的な質問 - 347
組み合わせと JRE - 339
属性をクラスに追加する - 327
低帯域幅の KVM 設定 - 284
電気的仕様 - 314
電源制御 - 11, 171, 373
読み取り/書き込み可能に設定できない状況 - 112
日付/時刻の設定 - 162, 222
入門 - 17
汎用ブレード シャーシの設定 - 176
標準マウス モード - 80
表示オプション - 90
物理的仕様 - 297
保守 - 227
有効な解像度 - 269
用語 - 12
留意事項 - 332

米国/カナダ/ラテン アメリカ

月曜日～金曜日
午前 8 時～午後 8 時 (米国東海岸時間)
電話 :800-724-8090 または 732-764-8886
CommandCenter NOC に関するお問い合わせ :6 を押してから 1 を押してください。
CommandCenter Secure Gateway に関するお問い合わせ :6 を押してから 2 を押してください。
Fax :732-764-8887
CommandCenter NOC に関する電子メール :tech-ccnoc@raritan.com
その他のすべての製品に関する電子メール :tech@raritan.com

中国

北京

月曜日～金曜日
午前 9 時～午後 6 時 (現地時間)
電話 :+86-10-88091890

上海

月曜日～金曜日
午前 9 時～午後 6 時 (現地時間)
電話 :+86-21-5425-2499

広州

月曜日～金曜日
午前 9 時～午後 6 時 (現地時間)
電話 :+86-20-8755-5561

インド

月曜日～金曜日
午前 9 時～午後 6 時 (現地時間)
電話 :+91-124-410-7881

日本

月曜日～金曜日
午前 9 時 30 分～午後 5 時 30 分
電話 : 03-5795-3170
電子メール :support.japan@raritan.com

ヨーロッパ

ヨーロッパ

月曜日～金曜日
午前 8 時 30 分～午後 5 時 (GMT+1 CET)
電話 :+31-10-2844040
電子メール :tech.europe@raritan.com

英国

月曜日～金曜日
午前 8 時 30 分～午後 5 時 (GMT)
電話 : +44(0)20-7090-1390

フランス

月曜日～金曜日
午前 8 時 30 分～午後 5 時 (GMT+1 CET)
電話 :+33-1-47-56-20-39

ドイツ

月曜日～金曜日
午前 8 時 30 分～午後 5 時 30 分 (GMT+1 CET)
電話 :+49-20-17-47-98-0
電子メール : rg-support@raritan.com

メルボルン (オーストラリア)

月曜日～金曜日
午前 9 時～午後 6 時 (現地時間)
電話 :+61-3-9866-6887

台湾

月曜日～金曜日
午前 9 時～午後 6 時 (標準時 : GMT -5、夏時間 : GMT -4)
電話 :+886-2-8919-1333
電子メール : support.apac@raritan.com